



## **Symantec Privileged Access Manager - 4.1.7**

# Table of Contents

<b>Release Information.....</b>	<b>30</b>
<b>Reference Architecture.....</b>	<b>30</b>
Foundation Functional Feature.....	30
Foundation Physical Architecture.....	35
<b>Installation Requirements.....</b>	<b>42</b>
<b>Supported Environments.....</b>	<b>43</b>
<b>Cryptography.....</b>	<b>48</b>
<b>Release Comparison.....</b>	<b>49</b>
<b>New Features in 4.1.7.....</b>	<b>50</b>
<b>New Features and Enhancements in Earlier 4.x Releases.....</b>	<b>52</b>
New Features in 4.1.6.....	52
New Features in 4.1.5.....	53
New Features in 4.1.4.....	54
New Features and Enhancements in 4.1.3.....	55
New Features and Enhancements in 4.1.2.....	57
New Features and Enhancements in 4.1.1.....	60
New Features and Enhancements in 4.1.....	61
New Features and Enhancements in 4.0.....	63
<b>Known Issues.....</b>	<b>66</b>
<b>Resolved Issues in 4.1.7.....</b>	<b>71</b>
<b>Resolved Issues in Earlier 4.x Releases.....</b>	<b>72</b>
Resolved Issues in 4.1.6.....	72
Resolved Issues in 4.1.5.....	73
Resolved Issues in 4.1.4.....	75
Resolved Issues in 4.1.3.....	75
Resolved Issues in 4.1.2.....	76
Resolved Vulnerabilities and Issues in 4.0.4.....	78
Resolved Issues in 4.1.1.....	79
Resolved Issues in 4.1.....	80
Resolved Issues in 4.0.3.....	80
Resolved Issues in 4.0.2.....	81
Resolved Issues in 4.0.1.....	83
Resolved Issues in 4.0.....	85
<b>New and Revised External API Calls in 4.x and 4.x.x Releases.....</b>	<b>86</b>
<b>Revised Credential Manager CLI Commands in 4.x Releases.....</b>	<b>95</b>
<b>Access Free PAM Training Videos From the IMS Software Academy.....</b>	<b>96</b>



<b>Related Products.....</b>	<b>98</b>
<b>Upgrading.....</b>	<b>99</b>
Upgrade Prerequisites for 4.1.7.....	100
Upgrade a Single Appliance to 4.1.7.....	105
Upgrade Appliances in a Cluster to 4.1.7.....	107
Upgrading Across a Multi-Site Cluster.....	110
Upgrade a Socket Filter Agent (SFA).....	116
Upgrade a Credential Manager A2A Client.....	116
Upgrade PAM SC Utility Appliances to Support PAM 4.1.x.....	120
<b>Introduction.....</b>	<b>122</b>
PAM (Network-Based) Access Control Overview.....	124
Credential Manager Overview.....	124
Credential Manager Components.....	125
Password Management and Requests.....	126
Credential Manager Password Flow.....	128
Application-to-Application (A2A) Credential Management.....	130
Secrets Management Overview.....	132
PAM Server Control (Host-Based) Access Control Overview.....	133
Threat Analytics Overview.....	133
<b>Deploying.....</b>	<b>136</b>
IP Addresses and Ports for Network Connectivity.....	137
Download PAM Installation Media.....	140
Deploy the VMware OVA Template.....	143
Deploy on an AWS Amazon Machine Image (AMI).....	146
Create AWS Objects.....	148
Configure Privileged Access Manager for AWS.....	151
Launch New AWS Instances (Optional).....	155
Connect to AWS Instances.....	156
Deploy a VHD on Microsoft Azure.....	157
Configure an Azure Connection.....	162
Clone a PAM Server Instance on VMware, AWS, or Azure.....	165
Deploy the Hardware Appliance.....	166
Configure Network Connections for the Appliance.....	173
Deploy the PAM Client.....	177
Configure How the Client is Made Available.....	183
Symantec PAM Client Silent Install.....	184
Symantec PAM Client Silent Uninstall.....	185
Use a Private Content Delivery Network to Distribute the PAM Client Installer.....	186
Ports Not Allowed for the Client.....	187

<b>Deploy the PAM Access Agent for Windows.....</b>	<b>188</b>
<b>How to Set Up a Cluster.....</b>	<b>194</b>
Cluster Deployment Requirements and Guidelines.....	196
Configure a Cluster.....	200
Add Sites to Your Cluster.....	202
Add a Member to a Site While the Cluster is Up.....	205
Change the IP Address of a Cluster Member.....	206
Tune a Cluster.....	207
Clustering Considerations for Appliances with Multiple Network Interfaces.....	207
Cluster Synchronization, Promotion, and Recovery.....	210
Primary Site Fault Tolerance.....	217
Configure Load Balancers to Determine the Availability of Cluster Nodes.....	217
<b>Install and Configure a Socket Filter Agent.....</b>	<b>217</b>
<b>Accessing PAM.....</b>	<b>223</b>
<b>Using PAM.....</b>	<b>226</b>
<b>Establish Connection Sessions and View Target Account Passwords.....</b>	<b>226</b>
Review the Access Page.....	226
Use the Limited Functionality Access Devices Panel on Standard Web Browsers.....	227
Use the Access Devices Panel from a Mobile Device.....	229
<b>Configure Your Account Settings.....</b>	<b>230</b>
Update Mobile User Password.....	232
<b>Display and Access Devices.....</b>	<b>233</b>
<b>Filter Views.....</b>	<b>236</b>
<b>View and Permit Views of Passwords.....</b>	<b>237</b>
<b>Set Up Java for Internet Explorer.....</b>	<b>237</b>
<b>Configuring a PAM Server.....</b>	<b>239</b>
Configure Global Settings.....	240
Configure RDP Proxy Service Settings.....	246
Default Administrator Accounts.....	246
Alternate Configuration Utility.....	247
Change Login for Config or Super User.....	248
Licensing and Product Usage Reporting.....	249
Configure Network Settings.....	251
Restrict Administrative Access.....	253
Additional Routes.....	254
Configure Container Network Settings.....	254
Custom Host File Entries.....	255
Authorize SNMP Polling.....	256
Add SNMP V3 Users.....	256

Enable SNMP Traps.....	256
Management Information Base (MIB) for SNMP Use.....	257
XCEEDIUM-MIB File.....	266
Configure Web Proxy Definitions.....	283
<b>Configure Security Settings.....</b>	<b>284</b>
Server Access Options Configuration.....	284
Secure Connections Using SSL Certificates.....	285
Create a Self-Signed SSL Certificate for Use in a Testing Environment.....	286
Obtain and Apply SSL Certificates for a Single-Server Production Environment.....	288
Obtain and Apply SSL Certificates for a Production Cluster.....	291
Extract Required Certificates and CRLs from a Single SSL Certificate.....	297
Certificate Revocation Update Options.....	303
Sign Java Applets.....	307
Delete a Certificate, CA Bundle, or CRL.....	307
Disable and Enable Cross-Site Scripting Attack Checking.....	308
Configure Enhanced Encryption for Stored Credentials.....	308
Configure SSH Proxy, SSH MindTerm, and TLS Cryptography Options.....	309
<b>Authenticate Users Logging in to the Server.....</b>	<b>310</b>
How to Set Up LDAP Servers for User Authentication.....	311
How to Configure Active Directory for User Authentication.....	314
Configure LDAP and RADIUS in Combination to Authenticate Users.....	316
How to Configure PKI Smart Card Authentication.....	317
How to Configure RADIUS or TACACS+ for Authentication.....	320
Configure PAM to Support RSA SecurID Authentication.....	322
Using SAML 2.0 to Authenticate Users.....	324
Configure PAM as a SAML Identity Provider (IdP).....	325
Configure PAM as a SAML Service Provider (SP).....	333
Azure AD as an Identity Provider (IdP).....	336
<b>Hardware Security Modules (HSMs) for Credential Manager.....</b>	<b>342</b>
Configure PAM to use a Safenet HSM.....	342
Configure PAM to use an Entrust nShield Connect or Connect XC HSM.....	345
Common HSM Features.....	350
<b>AWS Coordination.....</b>	<b>350</b>
<b>Configure and Manage Session Recording.....</b>	<b>354</b>
<b>Use Logs to Monitor Operations and User Sessions.....</b>	<b>360</b>
Purge Session Logs Automatically.....	361
Save or Purge Session Logs Manually.....	361
Configure an External MySQL Database for Session Logs (Optional).....	362
Configure a Splunk Server for Logging.....	363
Configure a Remote Syslog Server.....	365

Configure a Server Control User Activity Server.....	366
Troubleshoot User Interface Problems.....	367
<b>Diagnostics and Troubleshooting.....</b>	<b>369</b>
Configure and Obtain Diagnostic Logs.....	369
Configure Performance Graphs.....	372
Configure System Diagnostics, Maintenance, and Cluster Tuning Options.....	372
Networking Tools.....	374
<b>Set Up Email for Monitoring (Legacy).....</b>	<b>375</b>
<b>Microsoft Office 365 Configuration.....</b>	<b>375</b>
<b>Power, Reboot, and FIPS Mode Controls.....</b>	<b>376</b>
<b>Configure Date/Time Settings.....</b>	<b>378</b>
<b>Set Your Locale.....</b>	<b>381</b>
<b>Configure Custom Branding.....</b>	<b>382</b>
<b>Implementing Access Control.....</b>	<b>383</b>
<b>Configure Devices.....</b>	<b>386</b>
About Devices.....	387
Device Features.....	388
Discover Devices on Your Network.....	391
Device Setup.....	394
Import and Export Devices.....	399
Device Group Setup.....	402
Import LDAP Device Groups.....	404
Device and Device Group Management.....	408
Device Viewing.....	410
Set Up Access to a Target Device.....	411
Access Methods.....	411
Create TCP/UDP Services to Access a Device.....	414
Configure RDP Applications Templates.....	430
Configure Auto-Login for Windows RDP.....	431
Manage Command and Socket Filters.....	433
Set up Command Filters.....	433
Socket Filter Agent Support.....	437
Setting Up Transparent Login.....	440
SSH Connections.....	441
Set Up Transparent Login for RDP Servers.....	443
Import or Export Transparent Login Configurations.....	458
Configure Support for Citrix Virtual Apps Resources.....	458
<b>Configure Users.....</b>	<b>461</b>
User Roles.....	462
Import and Export Roles.....	468

Identify User Roles and Privileges.....	469
Create and Manage Users.....	474
Configure User Groups.....	479
Import LDAP User Groups.....	484
Import and Export Groups.....	490
Manage User Accounts.....	491
User Viewing.....	493
<b>Provision Access Policies.....</b>	<b>493</b>
Set Up a Policy.....	496
Import or Export Policies.....	499
Set Up an AWS Policy.....	501
Dynamic Addition of Devices and Target Accounts to the Access Page Based on Target Group Membership.....	501
Policy inspection.....	502
<b>Implementing Credential Manager.....</b>	<b>503</b>
Default Ports for Credential Manager.....	504
Credential Manager Operation Settings.....	508
Configure Email Preferences for Password View Policies.....	511
Specify a Target Server.....	521
Identify Target Applications and Connectors.....	522
Add an Active Directory Target Connector.....	525
Active Directory Target CLI Configuration.....	526
Active Directory Target Connector External API Configuration.....	530
Add an Active Directory SSH Key Target Connector.....	532
Active Directory SSH Key Target CLI Configuration.....	534
Active Directory SSH Key Target Application External API Attributes.....	536
Add an AWS Access Credentials Target Connector.....	538
AWS Access Credentials CLI Configuration.....	539
Add an Azure AD Target Connector.....	541
Add a BMC Remedy Target Connector.....	543
Add CA NIM Target Connectors.....	544
Add a Cisco Target Connector.....	544
Cisco Target CLI Configuration.....	546
Cisco Target Connector External API Configuration.....	554
Add an HP Service Manager Target Connector.....	562
Add an IBM i Target Connector.....	562
IBM i Target CLI Configuration.....	563
IBM i Target Connector External API Configuration.....	564
Add a Juniper Junos Target Connector.....	566
Juniper Junos Target CLI Configuration.....	566

Juniper Junos Target Connector External API Configuration.....	568
Add an LDAP Target Connector.....	570
LDAP Target Connector CLI Configuration.....	571
LDAP Target Connector External API Configuration.....	574
Add an MSSQL Target Connector.....	576
MSSQL Target Connector CLI Configuration.....	577
MSSQL Target Connector External API Configuration.....	578
Add an MSSQL Azure Managed Instance Target Connector.....	580
MSSQL Azure Managed Instance Target Connector CLI Configuration.....	581
MSSQL Azure Managed Instance Target Connector External API Configuration.....	582
Add a MySQL Target Connector.....	584
MySQL Target Connector CLI Configuration.....	585
MySQL Target Connector External API Configuration.....	586
Add an Oracle Target Connector.....	588
Oracle Target Connector CLI Configuration.....	588
Oracle Target Connector External API Configuration.....	592
Add a Palo Alto Target Connector.....	595
Palo Alto Target Connector CLI Configuration.....	597
Palo Alto Target Connector External API Configuration.....	601
Add a RADIUS/TACACS+ Secret Target Connector.....	605
Add a ServiceNow Target Connector.....	605
Office365 Integration Messages, SAML IdP and SP Messages.....	605
Add an SPML Target Connector.....	607
SPML Target Connector CLI Configuration.....	607
SPML Target Connector External API Configuration.....	609
Add a Sybase Target Connector.....	611
Upload a Sybase SDK JAR File for the Sybase Target Connector.....	612
Add the Sybase Target Application and Connector.....	612
Sybase Target Connector CLI Configuration.....	613
Sybase Target Connector External API Configuration.....	615
Add a UNIX Target Connector.....	616
UNIX Target Connector CLI Configuration.....	620
UNIX Target Connector External API Configuration.....	629
Add a VMware ESX/ESXi Target Connector.....	639
VMware ESX/ESXi Target Connector CLI Configuration.....	640
VMware ESX/ESXi Target Connector External API Configuration.....	641
Add a VMware NSX Controller Target Connector.....	643
VMware NSX Controller Target Connector CLI Configuration.....	644
VMware NSX Controller Target Connector External API Configuration.....	645
Add a VMware NSX Proxy Target Connector.....	647

VMware NSX Proxy Target Connector CLI Configuration.....	647
VMware NSX Proxy Target Connector External API Configuration.....	647
Add a WebLogic Target Connector.....	648
WebLogic Target Connector CLI Configuration.....	649
Add a Windows SSH Key Target Connector.....	651
Windows SSH Key Target Connector CLI Configuration.....	653
Windows SSH Key Target Connector External API Configuration.....	657
Add a Windows SSH Password Target Connector.....	663
Windows SSH Password Target Connector CLI Configuration.....	665
Windows SSH Password Target Connector External API Configuration.....	669
Add a Windows Remote Target Connector.....	675
Windows Remote Target Connector CLI Configuration.....	678
Windows Remote Target Connector External API Configuration.....	681
Add a Windows Proxy Connector.....	683
How to Install a Windows Proxy for Credential Manager.....	685
Add Windows Proxy Target Applications and Accounts.....	691
Windows Proxy Target Connector CLI Configuration.....	695
Windows Proxy Target Connector External API Configuration.....	698
View Windows Proxy Logs.....	700
API Key Target Connector.....	701
<b>Develop Custom Connectors for Remote Targets.....</b>	<b>701</b>
Deploy the Custom Connector Software.....	704
Sample server.xml File.....	712
Use an Alternate Custom Connector Server for Disaster Recovery.....	718
Use A2A to Secure the Keystore and Password (Optional).....	719
Try Out the Sample Custom Connectors.....	729
Learn How to Use the Custom Connector Components.....	734
UI Fields and Controls for Configuring Connectors.....	736
Web Service Endpoints for the Custom Connector.....	753
Build Your Custom Connector.....	758
Configure Custom Connectors Using the CLI.....	768
Troubleshoot Custom Connector Issues.....	770
<b>Configure SSH Key Pair Policies.....</b>	<b>773</b>
<b>Add Target Accounts to Target Applications.....</b>	<b>774</b>
Add Target Accounts using the CLI.....	778
Use Account Discovery to Add Target Accounts.....	783
Synchronize Target Account Passwords.....	786
Verify Synchronized Target Account Passwords.....	787
Schedule Password Updates and Verifications.....	789
Use an Alternate Account to Change Passwords (Optional).....	790

Configure Windows Remote Target Accounts.....	791
Configure MSSQL Target Accounts.....	793
Configure MSSQL Azure Managed Instance Target Accounts.....	794
Configure IBM i Target Accounts.....	796
Discover Active Directory Services and Scheduled Tasks.....	798
Cisco SSH Target Account Configuration.....	800
SSH Key Authentication for Accessing UNIX/LINUX Targets.....	804
Use SSH Key Discovery to Find Key Pairs.....	806
SSH Certificate Authentication for Accessing UNIX/LINUX Targets.....	811
Create an SSH Certificate Policy with the UI.....	814
Set the Privilege Elevation for UNIX Target Accounts.....	815
Oracle Target Account Configuration.....	815
Palo Alto Account Configuration.....	817
Configure Windows SSH Key Target Accounts.....	817
Configure Windows SSH Password Target Accounts.....	818
<b>Set Up Password Composition and View Policies.....</b>	<b>819</b>
Construct Password Composition Policies.....	819
Create a Password Composition Policy with the UI.....	821
Create a Password Composition Policy with the CLI.....	822
Establish Password View Policies.....	825
Create a Basic Password View Policy.....	826
Modify the Default Password View Policy.....	830
Configure Password View Policies That Require Approval of Requests.....	830
Require an Account Check-Out to View the Password.....	844
Enable Email Notifications for Viewed Passwords.....	850
Track Account Movement Across Active Directory OUs.....	851
See a List of Password View Requests.....	852
Make a Request to View a Password.....	852
<b>Configure Just in Time (JIT) Provisioning for MSSQL User Accounts.....</b>	<b>854</b>
Add the LDAP Domain Server Required for JIT Provisioning.....	855
Import LDAP User Groups for JIT Provisioning.....	856
Create a Device for the MSSQL Database That Requires JIT Provisioning.....	857
Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in.....	857
Create a Target Application for the MSSQL Database Admin Account Used by JIT Provisioning.....	859
Create a Target Account for the MSSQL Database Administrator (for JIT Provisioning).....	859
Configure a Provisioned Account for JIT Provisioning.....	860
Create a Password View Policy for the JIT Provisioned Account.....	860
Create a Target Application for the JIT Provisioned Account.....	860
Create a Target Account for the MSSQL JIT Provisioned Account.....	861
(Optional) Restrict Users from Editing RDP User Name Values.....	862



Create an Access Policy for JIT LDAP Users.....	862
User Experience: Just in Time (JIT) Checkout and Check-in Operations.....	863
<b>Configure Just in Time (JIT) Provisioning for Azure SQL Managed Instance User Accounts.....</b>	<b>863</b>
Add the LDAP Domain Server Required for JIT Provisioning.....	864
Import LDAP User Groups for Azure SQL JIT Provisioning.....	865
Create a Device for the Azure SQL Managed Instance That Requires JIT Provisioning.....	866
Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in.....	866
Provide an Administrator Account to Use to Access the Azure SQL Managed Instance for JIT Provisioning.....	868
Configure a Provisioned Account for Azure SQL Managed Instance JIT Provisioning.....	869
Create a Password View Policy for the JIT Provisioned Account.....	869
Create a Target Application for the JIT Provisioned Account.....	870
Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account.....	870
(Optional) Restrict Users from Editing Azure User Name Values.....	871
Create an Access Policy for Azure Managed Instance JIT LDAP Users.....	872
User Experience: Just in Time (JIT) Checkout and Check-in Operations.....	872
<b>Delegate Password Management Tasks to Groups.....</b>	<b>873</b>
Credential Manager Group Terminology.....	874
Add Credential Manager Target Groups.....	877
Add Credential Manager Requestor Groups.....	882
Manage Credential Manager Credential Groups.....	884
Add or Modify Credential Manager Roles.....	890
Configure Users with the Manage Credentials Privilege to View Passwords on the Access Screen.....	898
Configure a PAM User to View the Password History of Target Accounts.....	901
<b>Manage Credentials Between Applications (A2A).....</b>	<b>904</b>
Install and Activate an A2A Client on a Request Server.....	907
Uninstall the A2A Client.....	914
Target Aliases for A2A Target Accounts.....	915
Start or Stop an A2A Client.....	915
A2A Client Connection Security.....	916
Integrity Verification.....	916
Add A2A Requestors.....	918
Example Requestors.....	920
Configure A2A Authorization Mappings.....	922
View Unsuccessful A2A Client Requests.....	925
Run an Example Application.....	925
Modify the A2A Client Configuration File.....	926
How the A2A Client Configures Cache Credentials to Local Storage.....	928
View A2A Client Logs.....	928
Update an A2A Client Key.....	928
View A2A Client Status and Troubleshoot Connection Issues in a Cluster.....	929

Configure an A2A Client to Use Another Server.....	930
Configure A2A Client Failover in a Multisite Cluster.....	931
Configure A2A Client Event Polling.....	932
<b>Implementing Secrets Management.....</b>	<b>934</b>
<b>About Secrets Management and Roles.....</b>	<b>934</b>
<b>Administering Users, Vaults, and Secrets.....</b>	<b>936</b>
Managing Vaults.....	936
Managing Secrets.....	938
Managing Secret Types.....	940
<b>Configuring Secrets Authorization.....</b>	<b>941</b>
Managing Secret Authorizations (Mappings).....	942
Using Secret Groups for Authorization.....	942
<b>Implementing PAM SC.....</b>	<b>945</b>
<b>PAM SC Unification Overview.....</b>	<b>945</b>
Server Control Components in PAM.....	949
PAM Unified Server Control Functional Overview and Business value.....	953
Server Control Concepts.....	955
PIM/PAM SC Component Changes in PAM 4.0.....	955
Server Control Roles in PAM.....	956
How Server Control Works.....	956
Technical Specifications.....	957
<b>PAM SC Guided Workflows.....</b>	<b>957</b>
Guided Workflow: Migrate a PIM or PAM SC Environment to PAM.....	957
Guided Workflow: Migrate a PIM or PAM SC Environment with UNAB to PAM.....	959
Guided Workflow: Add a New PAM Server Control Implementation to PAM.....	961
<b>Install And Configure PAM SC Utility Appliances.....</b>	<b>963</b>
License PAM To Support Server Control.....	963
Download and Deploy a New Utility Appliance.....	963
Add Utility Appliances to an Existing Environment.....	964
Utility Appliance Ports for Network Connectivity.....	964
<b>Configure PAM to Communicate with Utility Appliances.....</b>	<b>965</b>
Configure PAM Devices for Utility Appliances.....	965
Add Utility Appliance Devices to Utility Groups.....	966
Locate Utility Appliance Devices and Utility Groups.....	967
Export and Import PAM SC Utility Appliance Devices and Device Groups.....	968
<b>Replace a Utility Appliance.....</b>	<b>969</b>
Deploy and Manage Utility Appliance Update Patches.....	970
View Utility Group Status.....	971
<b>Migrate From PIM or PAM SC to PAM.....</b>	<b>976</b>

Migrate Policy Management Data.....	976
Prepare to Migrate to PAM.....	976
Migrate Data from PIM or PAM SC to PAM on Windows.....	980
Migrate Data from PIM or PAM SC to PAM on Linux.....	983
How to Change the Migration Utility Timeout Value.....	986
How to Configure the Migration Utility to Work with a Copy of DMS Data.....	987
View Server Control Endpoint Agent Status on the Device Agent Status Screen.....	988
Post Migration Steps.....	991
Extract PIM Shared Account Management (SAM) Data.....	992
<b>Upgrade and Migrate PIM and PAM SC Endpoints.....</b>	<b>996</b>
Upgrade a Windows Endpoint.....	996
Upgrade an AIX Endpoint.....	997
Upgrade a Linux Endpoint.....	1005
Upgrade a Solaris Endpoint.....	1012
Upgrade a Solaris Zones Endpoint.....	1019
Migrate an Endpoint.....	1029
<b>Associating PAM SC Devices with PAM Devices.....</b>	<b>1031</b>
Manually Associating a PAM SC Device with a PAM Device.....	1031
Changing or Deleting the PAM SC Device Association.....	1031
Automatically Match PAM SC Devices with PAM Devices.....	1032
Associating Device Matches and Running the Device Match Operation.....	1033
Deleting Multiple PAM SC Device Associations.....	1033
<b>Install PAM SC Endpoints.....</b>	<b>1033</b>
Download the PAM SC Endpoint Installation Software.....	1033
Install and Uninstall UNIX PAM SC Endpoints Using YUM.....	1034
Install a PAM SC Endpoint on Windows.....	1037
Uninstall a PAM SC Endpoint from a Windows System.....	1039
Install a PAM SC Endpoint on a UNIX Host.....	1040
Use a Warning Period.....	1042
Security Implementation Tips.....	1043
UNAB Endpoint Post Installation Configuration.....	1045
<b>Server Control Configuration Settings.....</b>	<b>1047</b>
Enabling Server Control TLS Settings.....	1048
<b>High Availability.....</b>	<b>1052</b>
Configure Endpoints for High Availability.....	1052
Communication Encryption.....	1053
Uninstall HP-UX Package.....	1053
<b>Configure PAM SC to Protect Your Endpoints.....</b>	<b>1053</b>
Server Control Policy Management Operations.....	1053
Manage and Troubleshoot Server Control Policies.....	1053

Advanced Server Control Policy Management.....	1055
Server Control Policy Management APIs.....	1057
Configure Login Integration for a Server Control Endpoint.....	1057
Agent Status Interval.....	1058
Configure Server Control Login Settings.....	1058
Test the Login Integration for Server Control Endpoints.....	1061
Change the ActiveMQ Password.....	1061
Import PIM and PAM SC Active Directory Users into PAM.....	1061
Configure UNAB to Provide Access to UNIX Computers Using Active Directory.....	1062
UNIX Authentication Broker (UNAB) Overview.....	1063
Manage UNAB Login Authorization for Devices and Device Groups.....	1064
Configure a UNAB Host or Host Group.....	1067
Verify Policy Deployment from a UNAB Endpoint.....	1068
Manage Server Control UNAB Policies Using the PAM External API.....	1068
TIBCO Configuration in PAM.....	1069
<b>Administrate PAM SC.....</b>	<b>1069</b>
Endpoint Administration for UNIX.....	1069
Manage Endpoints.....	1070
PAM SC Safe User Substitution.....	1079
Define PAM SC SUDO Records.....	1082
PAM SC Tools for Preventing Password Attacks.....	1084
PAM SC Enhanced Access Restrictions for UNIX Files and Directories.....	1086
Block Trojan Horses with the _abspath Group.....	1092
PAM SC Synchronization with Native UNIX Security.....	1092
Monitor Sensitive Files.....	1094
Protect the Internal Files (UNIX).....	1094
Protect setuid and setgid Programs.....	1096
Kernel Modules Load and Unload Protection.....	1097
Protect Binary Files from the kill Command.....	1099
Control Login Commands.....	1099
Protect TCP/IP Services.....	1106
Policy Model Database (UNIX).....	1115
Dual Control.....	1131
Use the seagent and sepmdd Daemons.....	1135
Protect Idle Stations.....	1136
Protect Resources Using APIs.....	1138
Protect Against Stack Overflow STOP.....	1138
Security Levels (UNIX).....	1140
Security Categories (UNIX).....	1140
Security Labels (UNIX).....	1141

---

Audit Logs (UNIX).....	1143
Log Routing.....	1146
Migrate User Trace Filters.....	1149
Improve Performance.....	1150
UNIX Exits.....	1157
Interact with LDAP.....	1161
NIS Configuration.....	1162
Restricting Local Interprocess Communication over UNIX (LOCAL) Named Domain Sockets.....	1166
Protect Process being Attached by Other Processes.....	1166
Endpoint Administration for Windows.....	1166
Manage Endpoints (Windows).....	1167
Expand Native Security.....	1171
Components.....	1174
Users and Groups.....	1176
Where Information about Accessors Is Stored.....	1176
Guidelines for Managing Accessors in Enterprise Stores.....	1177
Database Accessors.....	1181
Classes.....	1185
Windows Services Protection.....	1191
Windows Registry Protection.....	1195
Protect File Streams.....	1197
Internal File Protection (Windows).....	1198
Manage PAM SC Authorization.....	1200
User Impersonation Protection.....	1204
Set Up the Surrogate DO Facility.....	1207
Define SUDO Records (Task Delegation).....	1207
Check User Inactivity.....	1211
Security Auditors.....	1212
Events Interception.....	1212
Warning Mode.....	1213
Monitor Access Control Activity.....	1216
What Privileged Access Manager Server Control Audits.....	1217
How Auditing Works for Interception Events.....	1223
View Audit Event Logs.....	1226
The Audit Log (Windows).....	1228
Group Authorization.....	1233
Ownership.....	1235
Authorization Examples.....	1236
Manage Sub Administrators.....	1239
Environmental Considerations.....	1240

---

Default Permissions to Access the Database.....	1241
Native Permissions to Access the Database.....	1242
Policy Model Database (Windows).....	1242
Automatic Rule-based Policy Updates.....	1246
Update Subscribers.....	1248
Mainframe Password Synchronization.....	1252
Toggle Driver Interception.....	1252
Disable CA Privileged Access Manager Server Control Kernel Interceptions.....	1253
Stack Overflow Protection.....	1253
Configure Settings.....	1255
Track User Behavior Activities on Server Control Endpoints Using an SIEM Tool.....	1255
<b>Troubleshoot PAM SC.....</b>	<b>1257</b>
View Server Control Policy Deployment Audit Data.....	1257
Troubleshoot Policies Deployed on Server Control Devices.....	1258
Troubleshoot Policies Deployed on Server Control Device Groups.....	1259
Troubleshoot Orphaned Data, Records, and Validation Errors.....	1260
Tune Performance.....	1263
General UNAB Troubleshooting.....	1264
Troubleshoot Policies Deployed on UNAB Devices.....	1271
Troubleshoot Policies Deployed on UNAB Device Groups.....	1272
Troubleshoot the Reporting Service.....	1273
General PAM SC Troubleshooting and Maintenance Procedures.....	1279
Install PAM Server Control Endpoints and Server Components.....	1288
Create Policies and Access Authorities.....	1304
Manage the CA Privileged Access Manager Server Control Database.....	1308
Connecting to Remote Computers.....	1309
Deploy Rules from a PMD.....	1311
Collect Audit Records.....	1312
<b>PAM SC reference.....</b>	<b>1315</b>
Configuration Files.....	1315
audit.cfg File Filter Audit Records.....	1315
auditrouteftl.cfg File Filter Audit Records Routing.....	1321
The accomon.ini File.....	1326
The Audit Log Route Configuration File selogrd.cfg.....	1332
kblaudit.cfg Filter Keyboard Logger Audit Records.....	1338
The lang.ini File.....	1340
The pmd.ini File.....	1344
The seos.ini Initialization File.....	1350
The UNAB Conflicts File.....	1402
The uxauth.ini File.....	1403

trcfilter.init.....	1412
Utilities.....	1412
acuxchkey Utility: Change Encryption Key Settings.....	1412
ChangeEncryptionMethod Utility: Change Encryption Method.....	1413
dbmgr Utility.....	1413
DictImport Utility: Import the Dictionary File.....	1421
dmsmgr Utility.....	1422
eACoexist Utility Detect and Register Coexisting Trusted Programs.....	1425
eACSigUpdate Utility Replace STOP Signature File.....	1434
eACSyncLockout Utility Synchronize Account Lockout.....	1434
issec Utility Display CA Privileged Access Manager Server Control Daemon Status.....	1435
ldap2seos Script Extract Users from LDAP for Adding into CA Privileged Access Manager Server Control.....	1435
seos2ldap Script Export CA Privileged Access Manager Server Control Users to LDAP.....	1436
ntimport Utility Import Windows Users and Groups.....	1437
policydeploy Utility Manage Enterprise Policy Deployment.....	1438
ReportAgent Utility Send Report Snapshots and Audit Events.....	1449
seaudit Utility Display Audit Log Records.....	1452
sebuildla Utility Create a Lookaside Database.....	1458
sechkey Utility.....	1460
seclassadm Utility Administer CA Privileged Access Manager Server Control Classes.....	1465
secompas Utility Compare Passwords.....	1467
secons Utility.....	1468
secrepsw Utility Create Policy Model and Shadow Files.....	1493
sedbpchk Utility Back Up the Database.....	1494
seerrlog Utility Display Error Log Records.....	1495
segrace Utility Display User Login Information.....	1495
seini Utility Manage Configuration Files.....	1498
seldapcred Utility Encrypt and Store a Credential.....	1501
seload Utility Load and Start CA Privileged Access Manager Server Control.....	1501
selogmix Utility Split and Merge Audit Log Files.....	1502
semsgtool Utility Maintain the Message File.....	1503
senable Utility Enable a Disabled User Account.....	1504
senone Utility Execute a Command as an Unauthorized User.....	1505
SEOS_load Utility Load the CA Privileged Access Manager Server Control Interception Module.....	1505
sepass Utility Set or Replace a Password.....	1506
AM SC sepmd Utility.....	1508
sepmdadm Utility Create PMDB Definitions.....	1515
sepropadm Utility Administer Database Properties.....	1517
sepromote Utility Enforce Strong Authentication.....	1518

sepuradb Utility Purge Database References to Undefined Records.....	1519
sereport Utility Reports Configuration.....	1519
seretrust Utility Generate Commands to Retruster Programs and Secure Files.....	1523
serevu Utility Handle Unsuccessful Login Attempts.....	1524
sesu Utility Substitute User.....	1525
sesudo Utility.....	1527
seuidpgm Utility - Extract Trusted Programs.....	1529
seversion Utility Display CA Privileged Access Manager Server Control Program Module Version Information.....	1530
sewhoami Utility Display Your PAM SC Server Control User name and Security Credentials on UNIX.....	1532
uninstall_AC Utility Remove CA Privileged Access Manager Server Control from the Current Computer....	1533
uxauthd.sh Script Administer UNIX Authentication Broker Agent.....	1534
uxauth_selinux.sh Enable SELinux Support.....	1535
uxconsole Utility Manage UNIX Authentication Broker Endpoints.....	1535
UxImport Utility Extract Information from the UNIX Operating System.....	1550
uxpatcher Utility.....	1552
Services and Daemons in Detail.....	1554
uxchecklogin Utility.....	1570
postupdate-nss-gr Utility.....	1572
Using the Sekmodutil Tool.....	1574
Audit Log Records.....	1576
Audit Event Types.....	1576
Audit Records.....	1600
Authorization Stage Codes for Inbound Network Connection Events.....	1602
Authorization Stage Codes for Log In and Log Out Events.....	1604
Authorization Stage Codes for Outbound Network Connection Events.....	1605
Authorization Stage Codes for Password Verification Events.....	1607
Authorization Stage Codes for Resource Access Events.....	1608
Authorization Stage Codes for Security Database Administration Events.....	1613
Authorization Stage Codes for Shutdown Events.....	1615
Authorization Stage Codes for Trace Message On a User.....	1616
Authorization Stage Codes for Untrust Message Events.....	1617
Reason Codes That Specify Why a Record Was Created.....	1618
selang Reference Guide.....	1618
Command Line Interpreter.....	1618
Features of the selang Command Shell.....	1620
selang Command Authorization.....	1624
selang Environments.....	1629
selang Configuration on UNIX.....	1630
Get selang Help.....	1631



Rules Effectiveness Exceptions.....	1632
selang Commands Reference.....	1632
selang Commands in the PAM SC Environment.....	1637
selang Commands in the Remote Configuration Environment.....	1714
selang Commands in the Native UNIX Environment.....	1717
selang Commands in the Native Windows Environment.....	1725
PAM SC selang Commands in the Policy Model Environment.....	1743
Classes and Properties.....	1749
Classes in the AC Environment.....	1750
Classes in the Windows Environment.....	1883
Classes in the UNIX Environment.....	1900
Classes for Custom Purposes.....	1901
Windows Values for PAM SC selang Commands.....	1901
String Matching.....	1905
Examples Wildcard Matching.....	1905
Character Lists.....	1906
Registry.....	1907
Build Number.....	1907
AccessControl.....	1907
agent.....	1909
Applications.....	1909
Client.....	1910
Common.....	1910
crypto (Windows).....	1915
Data.....	1916
Dependency (Registry Settings).....	1917
devcalc (Windows).....	1917
Exits.....	1917
FsiDrv.....	1919
Instrumentation.....	1922
lang Registry.....	1928
logmgr Registry.....	1929
message Registry.....	1931
OS_User.....	1931
passwd Registry.....	1932
pmd.....	1933
policyfetcher (Windows).....	1937
PUPMAgent Registry.....	1938
Report.....	1939
ReportAgent Registry.....	1939

SeOSD Registry.....	1940
SeOSWD.....	1945
STOP.....	1946
Tracer.....	1946
uxauth Key Registry Settings.....	1947
WebService.....	1947
Additional Registry Keys.....	1949
Trace Messages.....	1950
APIAUTH Messages.....	1950
CONNECT Messages.....	1952
ERROR Messages.....	1952
EXEC Messages.....	1954
FILE Messages.....	1955
INET Messages.....	1956
INFO Messages.....	1956
KILL Messages.....	1958
LOGIN Messages.....	1959
SCONSOLE Messages.....	1959
SGID Messages.....	1960
SHUTDOWN and STARTUP Messages.....	1960
SUID Messages.....	1961
WARNING Messages.....	1961
WATCHDOG Messages.....	1962
Other Trace Messages.....	1963
PAM SC Communication Ports.....	1965
PAM SC UNIX Endpoint Used Ports.....	1965
Windows Endpoint Used Ports.....	1967
Default TCP Ports Used by PAM SC Server Components.....	1967
UNIX Authentication Broker Used Ports.....	1968
Endpoint Management Used Ports.....	1969
ObserveIT Used Ports.....	1970
<b>PAM SC Frequently Asked Questions.....</b>	<b>1970</b>
<b>Implementing Threat Analytics.....</b>	<b>1976</b>
<b>Integrate Threat Analytics.....</b>	<b>1978</b>
Deploy the Symantec Threat Analytics Server.....	1979
Enable Threat Analytics Mitigation Actions.....	1988
Set up SAML Authentication (Optional).....	1989
<b>Configure Threat Analytics Using the Admin Dashboard.....</b>	<b>1991</b>
<b>Analyze User Activity and Analytics.....</b>	<b>1995</b>
Examine All Network Activity in Detail.....	2001

Monitor Risk Analytics.....	2003
Map User Locations.....	2005
Graph Network Resources.....	2006
Review Session Logs.....	2008
<b>Investigate Basic Components of the Network.....</b>	<b>2009</b>
Examine Users and Risk Levels.....	2009
Track Analytics for All Devices.....	2011
View All Analytics and Status Decisions.....	2012
Track Activity across All Services.....	2015
Monitor Activity Across All Resources.....	2019
Interpret Threats Using the Discover Tab.....	2021
View Data Insights on Network Activity.....	2025
<b>Track Risk Level Activity for All Users and Devices.....</b>	<b>2029</b>
<b>Configure Threat Analytics Console Settings.....</b>	<b>2035</b>
Manage Threat Analytics Users.....	2036
Select which Device Analytics Are Enabled or Disabled.....	2037
Select which User Analytics Are Enabled or Disabled.....	2038
Whitelist or Blacklist Users from Network Locations Based on Country.....	2039
Manually Identify Device Locations.....	2040
Manage Subnets.....	2042
Set Up SMTP for Email.....	2043
Configure Syslog/SIEM Logging.....	2044
Modify Analytic Configurations, Jobs, and Mixing Functions.....	2046
<b>Access User Activity Using IP Search.....</b>	<b>2050</b>
<b>Administrating.....</b>	<b>2055</b>
<b>Account Types.....</b>	<b>2055</b>
<b>Dashboards.....</b>	<b>2056</b>
Overview Dashboard.....	2056
System Dashboard (Single Node).....	2059
Management Console Cluster Dashboard.....	2064
<b>Session Management.....</b>	<b>2069</b>
View Session Logs and Reports.....	2070
View Session Recordings.....	2071
Manage Sessions By Specific Criteria.....	2074
<b>Display a Message to Users at Login.....</b>	<b>2075</b>
<b>Maintenance.....</b>	<b>2076</b>
Configuration and Database Backups.....	2077
Schedule a Backup of the Database.....	2078
Restore the Database from a Backup File.....	2081
Compact the PAM Database to Improve Startup Time.....	2082

Restore the Database to a New Appliance.....	2083
Hardware Appliance Backup and Recovery.....	2086
Backup the Hardware Appliance.....	2087
Recover a 404L Hardware Appliance.....	2087
Reset the Appliance to Factory Default State.....	2089
AWS AMI Backup and Recovery.....	2090
Mitigate Host Header Attacks.....	2092
Memory Management.....	2092
View System Information.....	2092
Cluster Maintenance.....	2094
<b>Credential Manager Reports.....</b>	<b>2096</b>
Available Credential Manager Reports.....	2096
Credential Manager Roles and Privileges for Running Reports.....	2102
Generate Credential Manager Reports.....	2104
Schedule Credential Manager Reports.....	2105
Credential Manager Activities List.....	2106
<b>Management Console.....</b>	<b>2107</b>
Add a Cluster to the Console.....	2110
Integrate with the Management Console.....	2112
Enable Console Services.....	2113
Upload Patches to the Console.....	2113
Cluster Details.....	2114
Stage a Patch Task.....	2116
View the Status of Tasks.....	2117
<b>Integrating.....</b>	<b>2118</b>
Configure Login Options for Windows Target Devices.....	2118
Configure Kerberos PIV/CAC Authentication for Windows Targets.....	2119
Kerberos Authentication Support in RDP Proxy Service.....	2121
VMware vCenter and NSX Integration.....	2121
NSX Provisioning Examples.....	2125
VMware NSX API Proxy Integration.....	2128
Managing Java on Your Client Workstation.....	2129
Juniper Integration.....	2130
Integrate a Java Application or Application Server.....	2131
Integrate with Your Service Desk Solution.....	2132
CA NIM UM and SM Integrations.....	2133
Clarity Service Desk Manager Integration.....	2133
HP Service Manager Integration.....	2136
BMC Remedy ITSM Integration.....	2139
ServiceNow Integration.....	2142

Salesforce Service Cloud Integration.....	2146
<b>Privileged Access Manager Server Control Login Integration.....</b>	<b>2148</b>
<b>Symantec SiteMinder Integration.....</b>	<b>2151</b>
<b>Integrate A2A Applications.....</b>	<b>2155</b>
<b>Integrate with SailPoint.....</b>	<b>2156</b>
<b>Programming.....</b>	<b>2160</b>
<b>PAM External REST API.....</b>	<b>2160</b>
Deploy the External REST API (Administrators).....	2161
Use the External REST API (Programmers).....	2165
External API Example Implementation.....	2168
Connect with SCIM API.....	2186
LDAP External REST API Extensions.....	2187
<b>Credential Manager CLI and Credential Manager Java API.....</b>	<b>2195</b>
Install and Set Up the Remote CLI and Java API.....	2195
Use the Credential Manager Java API.....	2199
Credential Manager Java API Example.....	2201
Use the Remote CLI.....	2215
Remote CLI Command Syntax.....	2215
Remote CLI Return Values.....	2216
Batch CLI Command Execution.....	2216
Credential Manager CLI Commands.....	2220
addAuthorization.....	2220
addFilter.....	2223
addGroup.....	2224
addPasswordPolicy.....	2225
addPasswordViewPolicy.....	2229
addRequestScript.....	2234
addRequestServer.....	2236
addRequestServerDefaults.....	2237
addRole.....	2238
addSSHKeyPairPolicy.....	2239
addTargetAccount.....	2239
addTargetAlias.....	2243
addTargetApplication.....	2244
addTargetServer.....	2246
addUser.....	2247
addUserGroup.....	2249
archiveAuditData.....	2250
archiveMetricData.....	2252
batchSequence.....	2253

canGetCredentials.....	2254
checkConnectionStatus.....	2255
checkDelete.....	2256
checkInAccountPassword.....	2256
deleteAuthorization.....	2256
deleteFilter.....	2258
deleteGroup.....	2259
deletePasswordPolicy.....	2259
deletePasswordViewPolicy.....	2260
deletePasswordViewRequest.....	2260
deleteRequestScript.....	2261
deleteRequestServer.....	2262
deleteRequestServerDefaults.....	2262
deleteRole.....	2263
deleteSSHKeyPairPolicy.....	2263
deleteSystemProperty.....	2264
deleteTargetAccount.....	2264
deleteTargetAlias.....	2265
deleteTargetApplication.....	2265
deleteTargetServer.....	2266
deleteUser.....	2267
deleteUserGroup.....	2267
disableCLIHostNameCheck.....	2268
disableFingerprinting.....	2268
enableCLIHostNameCheck.....	2268
enableFingerprinting.....	2268
enableLicense.....	2268
expirePasswordViewRequest.....	2269
forceCheckInAccountPassword.....	2269
generateEncryptedPassword.....	2270
getAllScriptHash.....	2270
getAwsManagementConsoleSessionUrl.....	2270
getErrorCodes.....	2272
getEventProcessingMetrics.....	2273
getLocalProperty.....	2273
getMostRecentPasswordHistory.....	2273
getMSOLFederatedSessionCmd.....	2274
getNumberOfAccounts.....	2276
getRequestServerDefaults.....	2276
getScriptHashAsynchronous.....	2276

---

getServiceStatus.....	2277
getSystemProperty.....	2278
listCurrentPasswordViewRequestSummary.....	2278
listDBCclusterMembers.....	2280
listPasswordViewRequestByAccount.....	2280
listPasswordViewRequestByApproverSummary.....	2282
listPasswordViewRequestByRequestorSummary.....	2285
listPasswordViewRequestSummary.....	2287
listRequestServer.....	2289
listRequestServerDefaults.....	2292
listUserAuthorization.....	2292
renameUser.....	2293
resetClientCache.....	2294
resetDBHash.....	2294
resetGroupCache.....	2295
searchAgent.....	2295
searchAuthorization.....	2297
searchFilter.....	2300
searchGroup.....	2301
searchPasswordPolicy.....	2303
searchPasswordViewPolicy.....	2304
searchPasswordViewRequest.....	2305
searchPasswordViewRequestByApprover.....	2309
searchPasswordViewRequestByRequestor.....	2312
searchRequestScript.....	2315
searchRequestServer.....	2316
searchRole.....	2318
searchSite.....	2319
searchSSHKeyPairPolicy.....	2320
searchTargetAccount.....	2321
searchTargetAlias.....	2324
searchTargetApplication.....	2325
searchTargetServer.....	2327
searchUser.....	2328
searchUserGroup.....	2329
setDisasterRecoverySettings.....	2331
setInitProperty.....	2332
setLocalProperty.....	2332
setPasswordViewReasons.....	2333
setPasswordViewRequestDeleteInterval.....	2333

---

setReportRowLimit.....	2334
setSystemProperty.....	2334
updateAgent.....	2341
updateAuthorization.....	2343
updateDBClusterMembers.....	2345
updateDBPassword.....	2346
updateFilter.....	2347
updateGroup.....	2348
updatePasswordPolicy.....	2349
updatePasswordViewPolicy.....	2353
updatePasswordViewRequestStatus.....	2357
updateRequestScript.....	2358
updateRequestServer.....	2360
updateRequestServerDefaults.....	2362
updateRequestServerKey.....	2363
updateRole.....	2364
updateServerKey.....	2365
updateSSHKeyPairPolicy.....	2365
updateTargetAccount.....	2366
updateTargetAccountDescriptor.....	2370
updateTargetAccountPassword.....	2371
updateTargetAlias.....	2373
updateTargetApplication.....	2374
updateTargetServer.....	2376
updateUser.....	2377
updateUserGroup.....	2379
updateUserPassword.....	2381
updateUserStatus.....	2381
verifyAccountPassword.....	2382
verifyDBHash.....	2382
viewAccountPassword.....	2383
Secrets Management CLI Commands.....	2385
addVault.....	2385
updateVault.....	2386
getVault.....	2388
deleteVault.....	2388
viewSecretPassword.....	2388
listVaults.....	2389
addSecret.....	2390
updateSecret.....	2392



getSecret.....	2394
listSecrets.....	2395
deleteSecret.....	2396
<b>Integrate Applications with the Credential Manager A2A Client.....</b>	<b>2396</b>
A2A Integration Return Data.....	2402
Integrate Java Applications with the Credential Manager A2A Client.....	2404
Integrate a Basic Java Application with the A2A Client.....	2404
Integrate a Standalone Java Application Using the A2A Client JDBC Wrapper.....	2408
Integrate a Java Application with the A2A Client on JBoss.....	2410
Integrate a Java Application with the A2A Client on Tomcat.....	2418
Integrate a Java Application with the A2A Client on WebLogic.....	2424
Integrate a Java Application with the A2A Client on WebSphere CE.....	2432
Integrate Apps to Use the Credential Manager A2A Client on UNIX and AIX.....	2439
Integrate a Perl Script with A2A Client on UNIX or AIX.....	2439
Integrate a C or C++ Application with A2A Client on UNIX or AIX.....	2441
Integrate a Korn Shell Script with A2A Client on UNIX or AIX.....	2443
Integrate a C Shell Script with A2A Client on UNIX or AIX.....	2444
Integrate a PHP Script with A2A Client on UNIX.....	2446
Integrate a Python Script with A2A Client on UNIX and AIX.....	2447
Integrate Apps to Use the Credential Manager A2A Client on Windows.....	2448
Integrate a Perl Script with A2A Client on Windows.....	2448
Integrate a Visual Basic Application.....	2449
Integrate a Visual C++ Application.....	2450
Integrate a C#.NET Application using IIS Application Server.....	2453
Integrate a Visual Basic, Java, or Windows Script.....	2456
Integrate a PowerShell Script with A2A Client on Windows.....	2460
Remote HTTP Interface to a Credential Manager A2A Client.....	2460
<b>Reference.....</b>	<b>2464</b>
<b>Privileged Access Manager Client Reference.....</b>	<b>2464</b>
<b>Data Formats.....</b>	<b>2465</b>
<b>Import and Export Data for Provisioning.....</b>	<b>2467</b>
Roles.....	2469
User Groups and Users.....	2469
Device Groups and Devices.....	2475
CSV Files for Services.....	2478
<b>Messages and Log Formats.....</b>	<b>2480</b>
Syslog Message Formats.....	2481
Syslog Priority Facility Severity Grid.....	2491
PAM-AGT: CA PAM Access Agent Messages.....	2492
PAM-CF: Connector Framework Messages.....	2493

---

PAM-CLNT: PAM Client Messages.....	2493
PAM-CM: Credential Manager Messages.....	2493
PAM-CMN: Common Messages.....	2501
General Error Messages.....	2502
Network Service Messages.....	2502
User Management Messages.....	2505
Smart Button Group Messages.....	2508
User Group Management Messages.....	2509
Device Management Messages.....	2509
Role and Privilege Messages.....	2514
Device Group Management Messages.....	2514
Global Settings and Device Task Messages.....	2515
LDAP Messages.....	2516
CSV Import/Export Related Messages.....	2517
Office365 Integration Messages, SAML IdP and SP Messages.....	2518
Policy Management Messages.....	2519
Management Console Messages.....	2520
Managed Server Service Messages.....	2521
Command and Socket Filter Messages.....	2521
Logging and Reporting Messages.....	2522
Policy Conflict Messages.....	2524
Authentication-Related Messages.....	2524
Access Service Messages.....	2528
Credential Management Messages.....	2529
View and Search Messages.....	2530
Cluster Management Messages.....	2530
Multi-Site Clustering Messages.....	2536
Login Sessions Management Messages.....	2540
Configuration Messages.....	2541
HSM Configuration Messages.....	2544
Secondary Transparent Login Messages.....	2546
AWS, VMware, and Azure Virtual Device Management Messages.....	2546
Credential Management API Non-Device Messages.....	2551
Session Recording Messages.....	2552
Session Manager Service Messages.....	2553
Upgrade, Backup, and Recovery Messages.....	2553
CA Threat Analytics Related Messages.....	2554
Active Directory Messages.....	2556
SAML Related Messages.....	2556
SSL, FIPS, and Cryptography Messages.....	2557

---

---

Other Common Messages.....	2559
Transparent Login Messages.....	2579
PAM-CS: Cluster Status Messages.....	2579
PAM-IMP: Import and Export Constants.....	2579
PAM-LDAP: LDAP Importer Messages.....	2580
PAM-MGC: Management Console Messages.....	2581
PAM-PAMSC: PAM SC Device Matching Messages.....	2585
PAM-PRX: Proxy Messages.....	2585
PAM-SP: SailPoint Messages.....	2586
PAM-SPFD: Secure Port Forwarding Daemon Messages.....	2587
PAM-SRM: Session Recording Manager Messages.....	2587
PAM-TELE: Telemetry Segment Messages.....	2589
PAM-UI: User Interface Messages.....	2589
PAM-UIL: UI Logging Messages.....	2596
PAM-UPD: Session Clean-up and Storage Status Messages.....	2596
Credential Manager Client Return Codes.....	2596
<b>Credential Manager Terms and Concepts.....</b>	<b>2629</b>
<b>Windows Shortcut Keys for the RDP Client.....</b>	<b>2631</b>
<b>Upgrade.....</b>	<b>2632</b>
<b>Third-Party License Acknowledgments.....</b>	<b>2634</b>
<b>Product Accessibility Features.....</b>	<b>2637</b>
<b>Important Links.....</b>	<b>2639</b>
<b>Telemetry Data.....</b>	<b>2640</b>
<b>Documentation Legal Notice.....</b>	<b>2642</b>

## Release Information

---

Release 4.1.7 contains **5** new features and resolves **42** issues.

### IMPORTANT

#### Functional Changes Related to Cluster Status and Remote Storage Emails

In previous releases, Cluster Status emails and Remote Storage emails were sent to the SMTP server defined on the **Configuration, Monitor (Legacy)** panel, which could be different on each node in the cluster.

In 4.1.7, all Cluster Status emails and Remote Storage emails are sent to the SMTP server defined on the **Configuration, Email Settings** panel, which is defined once on the primary node and replicated to all nodes in the database. You must therefore define the SMTP server in the **Email Settings** for the Cluster Status and Remote Storage Status emails to continue to be sent from any node.

The SMTP server that is specified in **Email Settings** must also be visible from all nodes in the cluster. Otherwise, Remote Storage emails (which alert the user when primary or failover remote storage is mounted, dismounted, or out of contact) are not sent from any node which cannot see the SMTP server.

**Known Issue:** Cluster Status notification emails for quorum loss events are not being sent. All other cluster status email notifications are working as expected.

#### Topics in this section:

- [Reference Architecture](#)
- [Installation Requirements](#)
- [Supported Environments](#)
- [Cryptography](#)
- [Release Comparison](#)
- [New Features in 4.1.7](#)
- [New Features and Enhancements in Earlier 4.x Releases](#)
- [Known Issues](#)
- [Resolved Issues in 4.1.7](#)
- [Resolved Issues in Earlier 4.x Releases](#)
- [New and Revised External API Calls in 4.x and 4.x.x Releases](#)
- [Revised Credential Manager CLI Commands in 4.x Releases](#)
- [Access Free PAM Training Videos From the IMS Software Academy](#)
- [Related Products](#)

## Reference Architecture

The topics in this section describe a Reference Architecture which provides information relating the baseline functional feature and technical architecture that is required to deliver the Privileged Access Manager foundational solution.

This artifact is relevant only to the implementation of the foundational solution. The artifact can be superseded by more detailed design, implementation, test, and operational artifacts. The following phases or iterations of the project illustrate how other artifacts support the maturation of the solution functionally and technically.

**Use the table of contents to access the topics in this section.**

## Foundation Functional Feature

This section contains the following topics:

- [Planned End State](#)
- [Solution Personas](#)
- [Interaction of Personas](#)
- [Foundation Capability Privileged Access Management](#)
- [Foundation Functional User Stories](#)

## **Planned End State**

The Planned End State is based on the solution requirements. The end state may be extended during the design process. This section documents the actors, processes, and walk-throughs of the "as-built" solution.

The PAM planned solution is summarized in the following table:

Solution Outcome	Description
Enhanced security governance and compliance	<ul style="list-style-type: none"> <li>• Stores passwords for managed privileged accounts</li> <li>• Credentials are encrypted using an AES 256 cipher before being stored for maximum security. A CMVP FIPS 140-2 validate cryptographic kernel, or use of a Hardware Security Module are optionally available</li> <li>• Manages privileged account password rotation according to the policies configured in accordance with customer requirements.</li> <li>• Employs a zero-trust posture to granting access to privileged accounts and devices. Access is granted only on a need-to-know basis.</li> <li>• Implements the following workflows to access account passwords:               <ul style="list-style-type: none"> <li>— Privileged account password request based on the approval workflow</li> <li>— Verification of user authentication every time a privileged account password is viewed</li> <li>— Access to privileged accounts based on an Administrator role</li> </ul>               When a user logs in to the Web Portal to access privileged accounts, one or more of the workflows takes effect depending on the job.             </li> <li>• Provides detailed Audit functions</li> <li>• Provided Session Recording</li> </ul>
Integration with existing corporate systems	<ul style="list-style-type: none"> <li>• Active Directory/LDAP and SailPoint integrations to help streamline the management of key data elements</li> <li>• Service Desk integrations to provide enhanced workflow</li> <li>• SIEM/Splunk/Syslog integration for consolidated activity reporting and searching</li> <li>• Federated authentication sources including PIV/CAC, RADIUS, and other protocols</li> </ul>

## **Solution Personas**

The following table summarizes the solution personas and how they can use the Privileged Access Manager solution. Where applicable, the personas that are listed represent the most common personas within Privileged Access Manager. Personas are grouped by the capability in which they play a role:

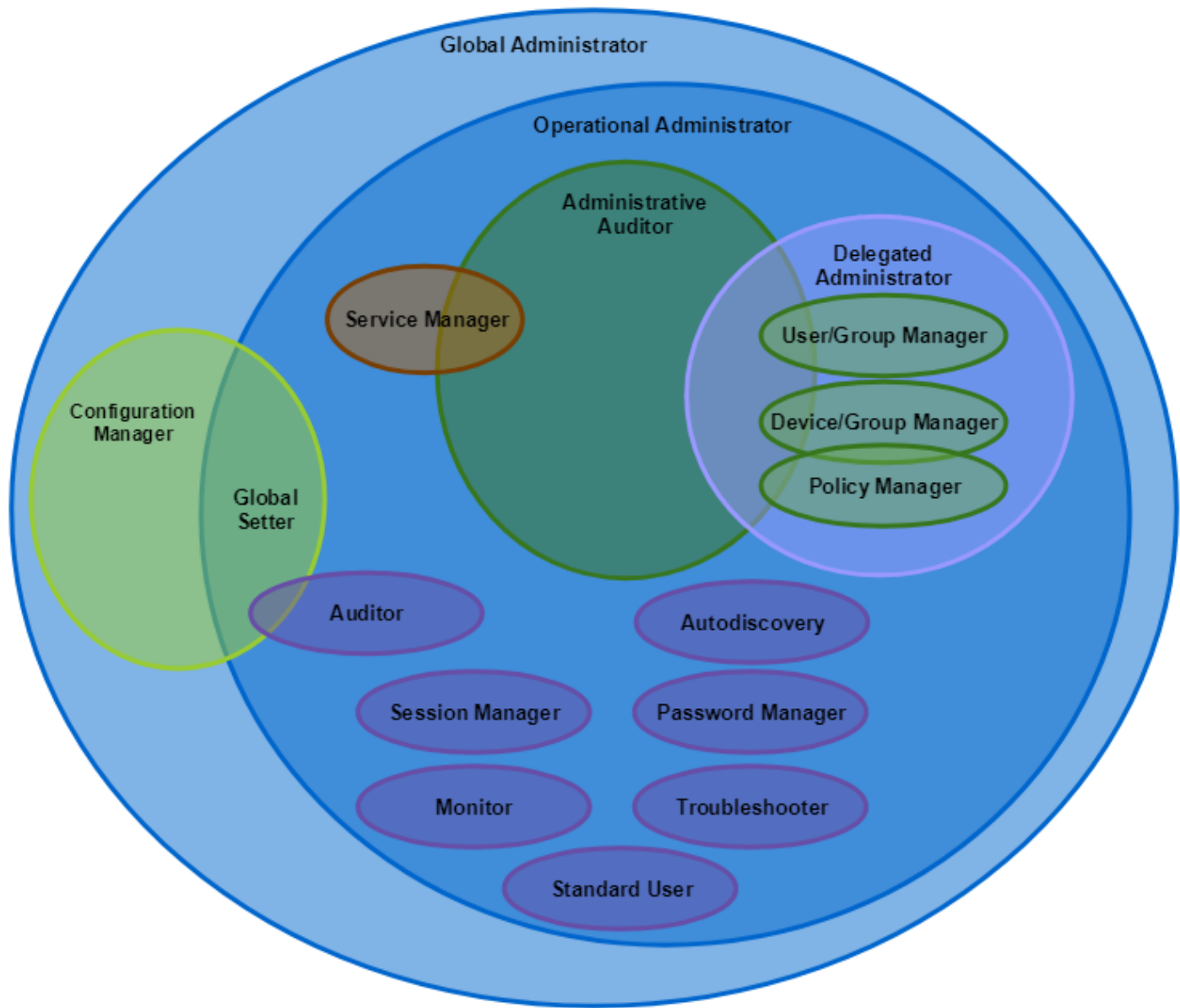
<b>Persona (Role)</b>	<b>Description</b>	<b>Expected Use of New Solution</b>
PAM Administrator	Administrator for PAM Solution	<ul style="list-style-type: none"> <li>• Manage the solution and solution configurations</li> <li>• Deploy and expand the solution footprint within the environment</li> <li>• Define which authorized end users/groups can access a Privileged ID password that is stored in the solution</li> <li>• Define which sets of end users/groups can access a solution-managed shared account</li> </ul>
PAM User	Individuals who are granted access to managed accounts and connect to the target devices through PAM.	<ul style="list-style-type: none"> <li>• Grant access to a Privileged ID using policies</li> <li>• Connect to the target/managed system using authorized privileged accounts</li> <li>• Depending on policy workflow, grants requests to reserve a privileged account password and releases when complete</li> </ul>
Access Approver	Individuals who approve/reject user requests to access managed accounts	Approves/rejects privileged password view requests submitted by the end user.
Security/Audit	Responsible for monitoring and reviewing security policies to ensure compliance with corporate standards and security levels	<ul style="list-style-type: none"> <li>• Review security policies</li> <li>• Review security events and reports</li> </ul>

## **Interaction of Personas**

Privileged Access Manager provides a preconfigured set of 17 roles that are mapped to the identified solution personas. This preconfigured set of privileges are required to perform various common activities. Roles are assigned to users and user groups when you configure or modify these objects.

The following Venn diagram shows the relationship of privilege and scope between the various out-of-the-box, predefined roles:

Figure 1: Venn Diagram of PAM Roles



The following list provides all the privileges that are assigned to each of the pre-configured roles shown in the previous graphic.

- **accessAll** : Global Administrator, Operational Administrator, Standard User
- **manageAll** : Global Administrator, Operational Administrator, Standard User
- **monitorAll** : Global Administrator, Monitor, Operational Administrator
- **sessionRead** : Global Administrator, Operational Administrator, Session Manager

- **sessionManage** : Global Administrator, Operational Administrator, Session Manager
- **overviewRead** : Auditor, Global Administrator, Operational Administrator
- **toolsAll** : Global Administrator, Operational Administrator, Troubleshooter
- **loggingAll** : Auditor, Global Administrator, Operational Administrator
- **sessionRecordingRead** : Auditor, Configuration Manager, Global Administrator, Global Setter, Operational Administrator
- **globalSettingRead** : Auditor, Configuration Manager, Global Administrator, Global Setter, Operational Administrator
- **globalSettingManage** : Configuration Manager, Global Administrator, Global Setter, Operational Administrator
- **servicesRead** : Administrative Auditor, Global Administrator, Operational Administrator, Service Manager
- **servicesManage** : Global Administrator, Operational Administrator, Service Manager
- **servicesDelete** : Global Administrator, Operational Administrator, Service Manager
- **usersRead** : Administrative Auditor, Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **usersManage** : Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **usersDelete** : Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **usersAssign** : Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **userGroupRead** : Administrative Auditor, Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **userGroupUpdate** : Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **cacUserApproval** : Delegated Administrator, Global Administrator, Operational Administrator, User/Group Manager
- **socketFilterAgentRead** : Administrative Auditor, Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator, Policy Manager
- **socketFilterAgentDelete** : Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator, User/Group Manager, Policy Manager
- **devicesRead** : Administrative Auditor, Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **devicesManage** : Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **devicesDelete** : Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **devicesAssign** : Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **deviceGroupRead** : Administrative Auditor, Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **deviceGroupUpdate** : Delegated Administrator, Device/Group Manager, Global Administrator, Operational Administrator
- **policyRead** : Administrative Auditor, Delegated Administrator, Global Administrator, Operational Administrator, Policy Manager
- **policyManage** : Delegated Administrator, Global Administrator, Operational Administrator, Policy Manager
- **socketFiltersRead** : Delegated Administrator, Global Administrator, Operational Administrator, Policy Manager
- **socketFiltersManage** : Delegated Administrator, Global Administrator, Operational Administrator, Policy Manager
- **commandFiltersRead** : Administrative Auditor, Delegated Administrator, Global Administrator, Operational Administrator, Policy Manager
- **commandFiltersManage** : Configuration Manager, Global Administrator, Operational Administrator, Policy Manager
- **policyImport** : Global Administrator, Operational Administrator
- **policyExport** : Global Administrator, Operational Administrator
- **configurationManage** : Configuration Manager, Global Administrator
- **rolesRead** : Administrative Auditor, Global Administrator, Operational Administrator
- **Autodiscovery** : Auto Discovery, Global Administrator, Operational Administrator
- **credentialsManager** : Global Administrator, Operational Administrator, Password Manager



**NOTE**

You can also download a [spreadsheet](#) that presents the privileges that are assigned to each pre-configured role in a matrix format.

**Foundation Capability Privileged Access Management**

The following table summarizes the capability, the technology, and the primary user stories.

Aspect	Description
Capabilities	<ul style="list-style-type: none"> <li>Controls the access of authorized users and other identities to elevated privileges across multiple systems that are deployed in an organization</li> <li>Provides secure access to target systems, over specific protocols, using the managed credentials, without the users knowing the credential</li> </ul>
Content/Enabling Technology	<ul style="list-style-type: none"> <li>Privileged Access Manager</li> </ul>
Primary User Stories	<ul style="list-style-type: none"> <li>Password Vaulting (Shared Account)</li> <li>Interactive Login Usage</li> <li>Account Access Approval</li> <li>Manage End-User Privileged Access</li> <li>Syslog Forwarding</li> <li>Self-contained, hardened appliance delivery</li> </ul>

**Foundation Functional User Stories**

The following table summarizes the functional user stories and the personas that participate in them.

As a...	I want to...	So that...
PAM Administrator	Define which authorized end users can access a stored Privileged ID password.	I control access to the Privileged ID in the password vault.
PAM User	Check out a Privileged ID.	I can access the target system interactively without needing to remember the system password
PAM User	Request access to a Privileged ID	I have temporary access to a target device after my request is approved.
PAM User	View a credential of a privileged account.	I have access to see the credential of the target account.
Access Approver	Certify an end-user request for a Privileged ID.	I can approve only authorized requests to access Privileged ID passwords
Security/Auditor	Review audit events and reports.	I ensure compliance with corporate standards and security levels

**Foundation Physical Architecture**

This topic details the default configuration requirements for applications. Requirements can include port numbers for web services, database configuration, OS configuration, and supporting services. The information aligns with the associated baseline technical architecture, focusing on specific platform requirements and component configurations for the Privileged Access Manager solution.

## Foundation Logical Architecture

The following architecture graphics illustrate the most common, logical components when working with Privileged Access Manager.

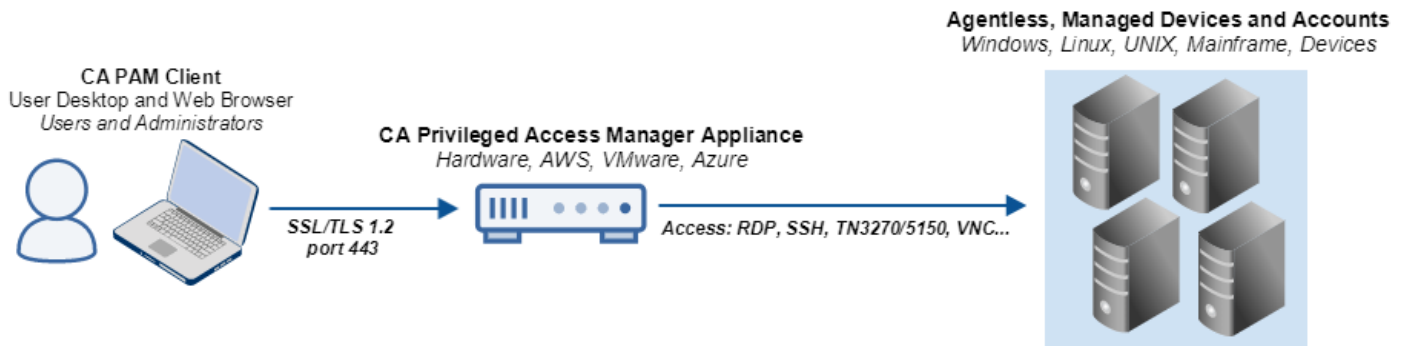
### NOTE

The only required logical architecture is a Privileged Access Manager appliance and a managed endpoint.

### Minimal Architecture

The following graphic shows a minimum architecture:

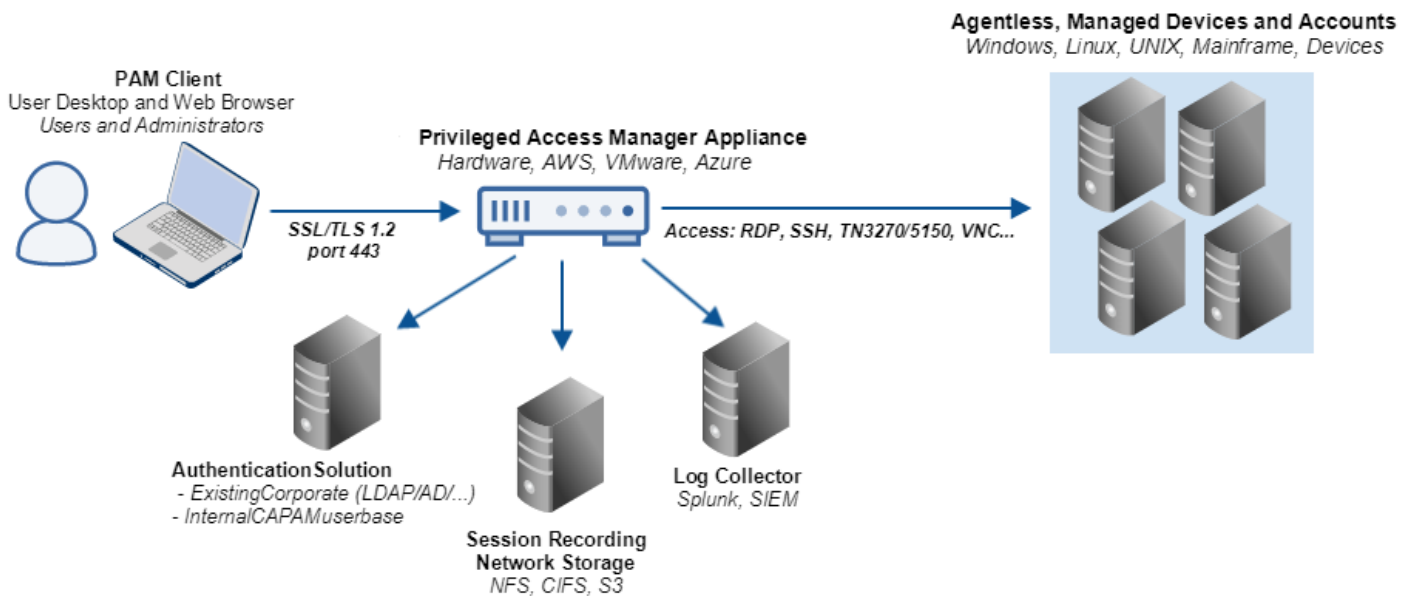
**Figure 2: Minimal PAM architecture**



### Advanced Architecture

The following graphic shows an advanced architecture:

**Figure 3: Advanced PAM Architecture**



## Solution Delivery

Privileged Access Manager is delivered as a self-contained, hardened appliance in the following forms:

- Physical hardware instance
- VMware - OVA
- AWS - AMI
- Azure - VHD

A single appliance contains all the necessary components to control privileged access in an environment.

Each appliance is a hardened appliance, which means that security measures are implemented to prevent any access to the appliance. All required configuration changes are available through the UI. Network tools are available to troubleshoot issues, such as firewall configurations.

In the rare case that a customer needs access, Broadcom Support is engaged to assist the customer in this task. This security posture prevents the on-site PAM Administrators from updating the appliance without an audit trail.

## Clustering

Appliances can be clustered together to satisfy *high availability*, *redundancy*, and *disaster recovery* requirements.

Privileged Access Manager supports clustering over a LAN and a WAN, under specific configurations. Administrators have the option of using single site clustering or multi-site clustering. Each cluster site is a logical grouping of PAM instances, which we recommend you deploy in a single data center.

### Single-and Multiple-Site Clusters

Configure a *single-site cluster* or *multi-site cluster* using the following guidelines to help determine which best suits your requirements:

- **Separation of administrative and access tasks:** To designate specific PAM nodes to handle global administrative functions (such as policy maintenance and credential rotation) and others to handle user requests for access to privileged devices, configure a [multi-site cluster](#). Address all administrative requests to the VIP of the Primary site and all access requests to the VIPs of Secondary sites.
- **Geographical distribution of data centers:** If all your PAM nodes are deployed at a single geographical location and you do not need to separate them for administrative and access tasks, you only require a [single-site cluster](#). If your PAM servers are deployed over multiple geographically dispersed locations, configure a [multi-site cluster](#).

### Single-Site Clusters

If all your PAM infrastructure is deployed at a single geographical location and you do not require separate administrative and access tasks between nodes, you only require a *single-site cluster*. PAM replicates data across all the nodes so that they operate as a single virtual system addressed by a single VIP.

#### NOTE

When you add another site to a single-site cluster, the first site you configured becomes the *Primary site* for the new multi-site cluster.

### Multi-Site Clusters

If your PAM environment is deployed over multiple geographically dispersed locations or if you want to designate specific nodes to handle administrative activities (recommended), configure a *multi-site cluster*. Each site in a multi-site cluster should contain at least two members. Multi-site clusters have one *Primary* site and one or more *Secondary* sites. Each site is addressed by its own VIP.

- **Primary site** members are co-located and are typically designated for administrative activities (policy maintenance, credential rotation). If user requests for access to privileged devices must also be handled at the same data center, create and designate a secondary site at the same location for that purpose. Data that is saved on one member of the Primary site is synchronously replicated across all Primary site members. Only one Primary site exists within a cluster at any time.

**NOTE**

The Primary site in a multi-site cluster behaves the same as a single-site cluster with the same properties. Primary sites and single-site clusters both use group replication to keep themselves in sync.

- **Secondary sites** are typically designated for access activities, that is, handling user requests for access to devices. Asynchronous replication is performed from the Primary site to Secondary sites. Replication allows Secondary site members to recover gracefully and continue operating should a network issue exist between the sites, like a brown-out or DC outage.

**NOTE**

A Secondary site can also be promoted to Primary site status, providing a warm backup if the Primary site goes down. For more information, see [Cluster Synchronization, Promotion, and Recovery](#).

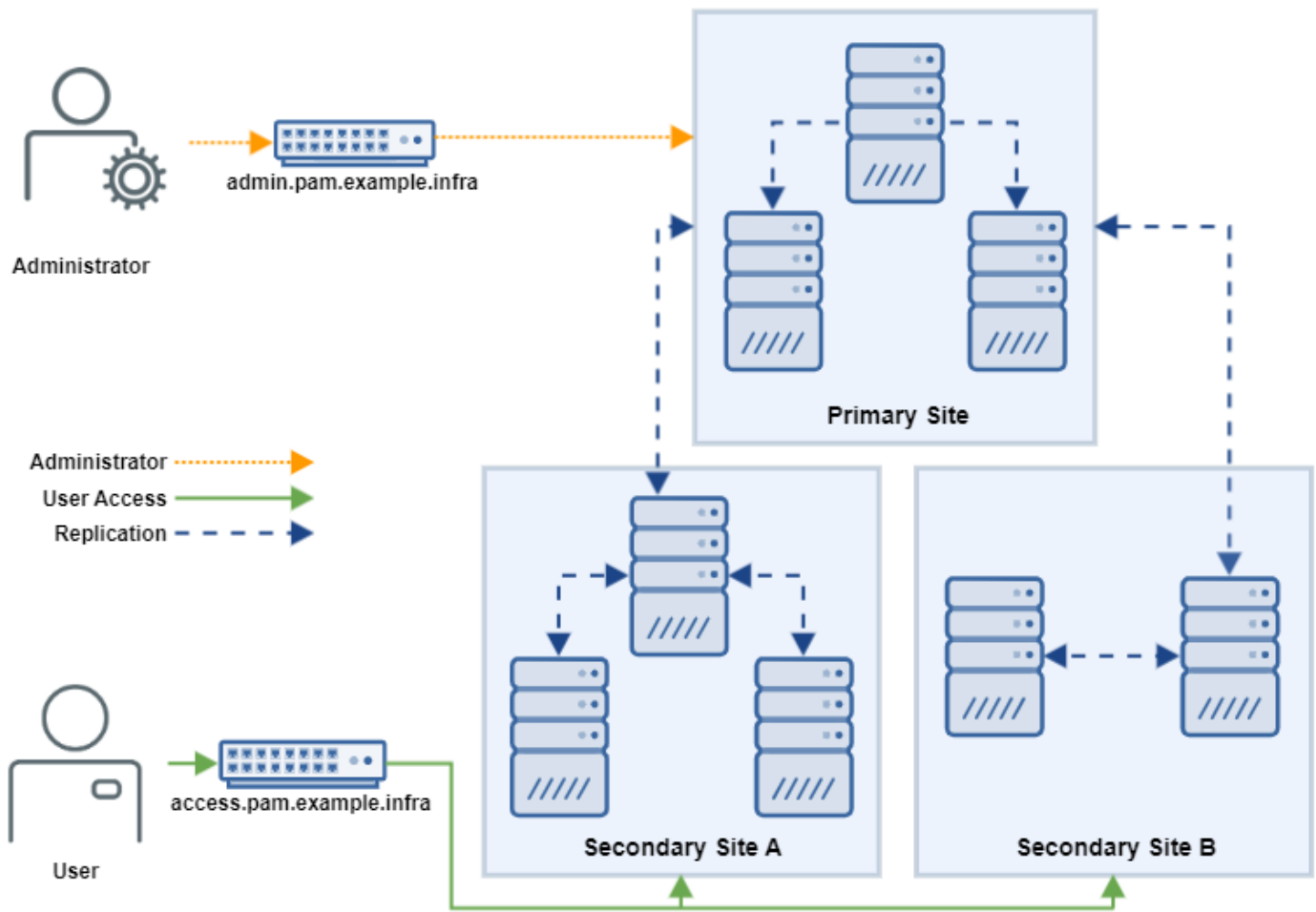
Sizing of a cluster is important and should be considered with customer corporate policies and procedures.

- **Primary site:** Three are recommended, with maximum of nine.
- **Secondary sites:** The number of sites can vary. At least one site per data center and two members per site are recommended.

For more information, see [Set Up a Cluster](#).

**Network Context*****Network Diagram – Foundation Physical Architecture***

The following diagram provides a reference implementation architecture design for the deployment of the Privileged Access Manager solution.

**Figure 4: Network Diagram - Foundation Physical Architecture****Foundation System Specification Requirements**

The specifications and requirements for the solution are defined in the following subsection.

Note the following information about sizing:

- Hardware-based PAM depends on third-party vendor specifications which is subject to change at any time
- Virtual based PAM (OVA, AMI, VHD) has required minimum specification for production grade systems

**Foundation Specification Architecture**

The minimum specification that is required for the Foundation Physical Architecture solution is given in the following table:

Node	Product, Versions, Options	Platform, OS, SP Level, Kernel Version	Memory, CPU, Processor, Speed, NIC Cards	Minimum Disk Space	Number Required (Recommended)
PAM	PAM 4.0	Hardened, Encrypted Linux	Memory: 16 GB Processor: 4 x Dual Core NIC: 1 – 1 GB	Recommended storage space for VM is 80 GB, however more is possible.	1 (4 - 2x2)
PAM Windows Proxy Server	PAM Windows Proxy Server	Windows 2012 R2 SE	Memory: 4 GB Processor: 2 x Dual Core		Optional, 2
NFS or CIFS Mount*		Windows 2012 R2 EE / Linux		500 GB – high network bandwidth; SSD preferred	2 per data center

\*NFS or CIFS mount is required for session recording data.

## Base System Configuration Requirements

### Node Configuration

No configuration of the appliances is required before installation. However, obtaining an appliance-specific license file is required.

### Solution Component Ports

All inbound traffic to PAM is over 443/TLS. The following table summarizes the outbound ports. For a comprehensive list of network ports for proper appliance functionality, see the [IP Address and Ports for Network Connections](#).

Source	Destination	Default Port	Port Type	Deployment Port	Other Comments
PAM	Windows Server	443	TCP	443	Windows Server connectivity with PAM Proxy – HTTPS
PAM	5250 Server	992	TCP	992	Credential Management – 5250 hosts
PAM	SMTP Server	25	TCP	25	SMTP Email Alerts
PAM	Windows Server	3389	TCP	3389	RDP Access
PAM	Syslog Servers	514	TCP	514	Syslog forwarding
PAM	Active Directory Instance	389	TCP	389	Active Directory Authentication
PAM	Active Directory Instance	636	TCP	636	Credential Management on Active Directory
PAM	CIFS Mount	139, 445	TCP	139, 445	Store for Session Recording
PAM	PAM Windows Proxy	135, 445, 27077	TCP	135, 445, 27077	WMI RPC

PAM Windows Proxy	PAM	443	TCP	443	PAM Windows Proxy
-------------------	-----	-----	-----	-----	-------------------

### Integrations

Privileged Access Manager integrates with many existing solutions and partners. The following table lists the most common components. Consult the **Configuration** section in the UI for a comprehensive list.

Component	Solution/Partner
Authentication	<ul style="list-style-type: none"> <li>• CA Single Sign On/SiteMinder</li> <li>• RSA</li> <li>• RADIUS</li> <li>• LDAP</li> <li>• Kerberos</li> <li>• PIV/CAC</li> <li>• SAML</li> </ul>
Auditing/Searching	<ul style="list-style-type: none"> <li>• Splunk</li> <li>• Syslog</li> <li>• SIEM</li> </ul>
APIs	<ul style="list-style-type: none"> <li>• Privileged Access Manager API/CLI</li> <li>• VMware NSX API</li> <li>• AWS APIs</li> </ul>
Cloud/Virtualization providers	<ul style="list-style-type: none"> <li>• VMware vCenter</li> <li>• AWS Management Console</li> <li>• Office 365</li> </ul>
Cryptography strength	<ul style="list-style-type: none"> <li>• OpenSSL</li> <li>• FIPS 104-2 compliance</li> <li>• HSM integration (onboard or from a third-party service)</li> </ul>
External Load Balancers	Health check-based balancing
Governance	<ul style="list-style-type: none"> <li>• CA Identity Management and Governance (IMAG)</li> <li>• SailPoint</li> </ul>
Service Desk	<ul style="list-style-type: none"> <li>• Remedy Service Desk</li> <li>• CA Service Desk</li> <li>• HP Service Manager</li> <li>• ServiceNow</li> <li>• Salesforce</li> </ul>
Secrets Management	Application-2-Application (A2A) for execution-time retrieval of credentials

### Common Configurations

The following table lists common configuration choices:

Business Function	Available Solutions
Authentication	Configure authentication for an existing customer implementation, using one of the various out-of-the-box options.

Users and user group membership management	In PAM, a policy matches a user or user group to a device (endpoint) or group of devices. Eliminate operational overhead by configuring users and their membership into user groups. Use Governance tools, such as CA IMAG or SailPoint, or using Active Directory/LDAP groups. When you manage users with these tools, they are automatically authorized and granted access to the appropriate devices and accounts in PAM.
Syslog/Splunk/SIEM integration	Access and Administration events are logged and available for audit purposes and can be sent to a third-party log aggregator. From the aggregator, customers generally adjoin PAM event information with events from other corporate systems to describe accurately user activity.
External Load Balancing	PAM provides a health check URL that informs load balancers whether an instance of PAM can receive traffic. <b>Note:</b> PAM is not a traditional n-tier application. Different use cases have caveats regarding when and how to use external load balancers. Also, external load balancers do not replace how and when the site-based VIPs are used within a PAM clustering configuration.

## Installation Requirements

Ensure that the following requirements are met before installing Privileged Access Manager.

### **Software Compatibility**

Before you upgrade, ensure that your existing installation is running a release and patch that you can upgrade to the current release. Verify whether you can upgrade by reviewing [Upgrading](#).

### **Hardware Appliance**

We have no special requirements for installing a Privileged Access Manager hardware appliance. Only general standalone computer hardware requirements apply.

The latest hardware appliance ships with 4 CPU cores (8 threads), 64 GB of RAM, and two 240 GB SSD. The appliance has 8 RJ45 network ports, and an expansion slot for a PCI card for HSM.

### **Virtual Instances**

Privileged Access Manager provides virtual images as VMware OVA, AWS AMI, and Azure VHD. When you provision these instances, we *recommend* the following parameters:

- Memory: 64 GB
- CPU: 8 cores (we support up to 512 CPU cores)
- Storage: 80 GB
- Disk Type: SSD

At a *minimum*, we require the following parameters:

- Memory: 16 GB
- CPU: 8 cores (we support up to 512 CPU cores)
- Storage: 80 GB
- Disk Type: SSD



**VMware OVA Instance**

One network interface is provided. Add extra required interfaces before its initial boot.

**AWS AMI Instance**

AWS specifications vary by region and over time. We suggest an AWS instance type of C4.4xlarge for production. For evaluation or testing, an instance type of M3 Medium is sufficient.

**Azure VHD Instance**

Azure specifications vary by region and over time. We suggest Azure size DS13 Standard for production. For evaluation or testing, an instance type of F2S Standard is sufficient.

## Supported Environments

**Deprecated Platform**

The Microsoft® Windows 2012 R2 platform is no longer supported for the PAM client.

**New Platforms**

Support for Windows 2022 and Red Hat 9 has been added in this release.

**At a Glance**

This content shows platform support for this version of the product. PAM ships as either a hardware or software-based appliance. In both cases, the operating system and database are included with the software package. We support the listed platforms for end-point Session Management, Credential Management, and ancillary agents. These agents (A2A Client, Socket Filter Agent, or PAM Workstation Client) are required for certain features of PAM.

The PAM Client is the recommended method for accessing the PAM UI. Various browsers, such as Chrome, Safari, Edge and Firefox can also be used with the following limitations:

- Microsoft Edge running in Internet Explorer mode is the only browser that still supports NPAPI, which is required for the device access applets. To use Microsoft Edge running in Internet Explorer mode, Java 8u-latest must be installed on the desktop.
- Microsoft Edge running in Internet Explorer mode does not support the [System Dashboard](#) or the [Management Console Cluster Dashboard](#).

**Session and Credential Management Platform Support**

Operating System Platforms	Supported?
IBM® AIX 7.2	✓
IBM® AIX 7.3	✓
Microsoft® Windows 10	✓
Microsoft® Windows 11	✓
Microsoft® Windows 2016	✓
Microsoft® Windows 2019	✓
Microsoft® Windows 2022	✓
Oracle® Solaris 11	✓
Red Hat® Enterprise Linux 7	✓

Operating System Platforms	Supported?
Red Hat® Enterprise Linux 8	✓
Red Hat® Enterprise Linux 9	✓
SuSE® Linux Enterprise Server 12.3-5	✓
SuSE® Linux Enterprise Server 15.0-2	✓

Databases (as Target Applications)	Supported?
IBM® DB2 v10.5 <sup>1</sup>	✓
IBM® DB2 v11.1 <sup>1</sup>	✓
IBM® DB2 v11.5 <sup>1</sup>	✓
MariaDB	✓
Microsoft® SQL Server 2014	✓
Microsoft® SQL Server 2016	✓
Microsoft® SQL Server 2017	✓
Microsoft® SQL Server 2019	✓
Oracle® 12c	✓
Oracle® 19c	✓
Oracle® 21c	✓
Oracle® MySQL 5.7	✓
Oracle® MySQL 8.x	✓

<sup>1</sup> IBM® DB2 is an OS credential. Use the UNIX connector. See product documentation.

Network Devices <sup>2</sup>	Supported?
Cisco™ ASA	✓
Cisco™ IOS	✓
Cisco™ TACACS+ Server	✓
Palo Alto PAN Server 6	✓
Palo Alto Devices (Layer 3, Option C configuration)	✓
Devices with *nix Operating Systems using SSHv2 connection	✓

<sup>2</sup> As Target Applications. Typically network devices use SSH protocol for user session establishment. Use the UNIX connector. See product documentation.

Mainframe <sup>3,4</sup>	Supported?
ACF2™ r15	✓
ACF2™ r16.0	✓
TopSecret® r15	✓
TopSecret® r16.0	✓

<sup>3</sup> Requires Broadcom LDAP for Mainframe System z/OS.

<sup>4</sup> Transparent Login functionality for Mainframe not supported.

Directories	Supported?
Symantec Directory v12	✓
Symantec Directory v14	✓
Microsoft® Active Directory <sup>5</sup>	✓
OpenLDAP v3 compliant	✓

<sup>5</sup> For any supported Windows Server.

Cloud & Virtualization Platforms	Supported?
Amazon Web Services™ Admin web console access	✓
Microsoft® Azure	✓
Microsoft® Office 365 Admin console access	✓
VMware vCenter 6.x	✓
VMware vCenter 7.0	✓

Web/Application Servers	Supported?
Apache Tomcat 7	✓
Apache Tomcat 8	✓
Apache Tomcat 9	✓
Oracle® Weblogic 10	✓

Threat Analytics (for PAM)	Supported?
Threat Analytics (for PAM) v2.3	✓
Threat Analytics (for PAM) v2.4	✓

IT Service Management Systems	Supported?
Service Desk Manager 14.1	✓
Service Desk Manager 17.0	✓
BMC Remedy 8.1	✓
BMC Remedy 9.1	✓
HP Service Manager 9.32	✓
HP Service Manager 9.41	✓
Salesforce Service Cloud (Winter 2015)	✓
ServiceNow (Istanbul)	✓
ServiceNow (Jakarta)	✓

## **PAM Client**

The PAM Client enables you to log in to PAM and perform administrator and end-user activities without a customer-installed web browser and Oracle Java engine. The Client removes the required maintenance of keeping Java and browser configurations compatible with PAM. You can run any PAM connection applets and can provide a complete substitute for the traditional PAM GUI using the Client.

The PAM Client is the recommended method for accessing the PAM UI. Various browsers, such as Chrome, Safari, Edge and Firefox can also be used with the following limitations:

- Microsoft Edge running in Internet Explorer mode is the only browser that still supports NPAPI, which is required for the device access applets. To use Microsoft Edge running in Internet Explorer mode, Java 8u-latest must be installed on the desktop.
- Microsoft Edge running in Internet Explorer mode does not support the [System Dashboard](#) or the [Management Console Cluster Dashboard](#).

You can download and install a PAM client version compatible with your workstation OS type from a button on the PAM GUI login page. The embedded JRE is downloaded with the client but PAM-served JARs download at runtime.

For MacOS, both Intel and ARM64 packages are provided.

PAM supports all versions of Linux supported by vendors.

<b>PAM Client (End-User Desktop Support)</b>	<b>Supported?</b>
Microsoft® Windows 10	✓
Microsoft® Windows 11	✓
Microsoft® Windows 2016	✓
Microsoft® Windows 2019	✓
Microsoft® Windows 2022	✓
Linux	✓
Apple macOS Big Sur	✓
Apple macOS Monterey	✓
Apple macOS Ventura	✓

## **PAM Access Agent**

The PAM Access Agent is a lightweight Windows alternative to the PAM Client.

<b>PAM Agent (End-User Desktop Support)</b>	<b>Supported?</b>
Microsoft® Windows 10 64-bit	✓
Microsoft® Windows 11 64-bit	✓

## **Mobile Support for PAM**

PAM offers limited support for mobile devices. The PAM browser user interface is optimized for password view requests and password check-in and check-out operations for mobile devices.

PAM supports Chrome browser on Android and Safari browser on iOS.

**PAM A2A Client**

A2A integration allows administrators to provide authorization for applications to access privileged credentials for application to application transactions. An A2A client is installed on the Request server where the requesting application resides and has various security checks to maintain authorization control. Multiple programming and scripting languages can be used (see product documentation for integration details).

PAM A2A Client	Supported?
IBM AIX 7	✓
Microsoft® Windows 10	✓
Microsoft® Windows 11	✓
Microsoft® Windows 2016	✓
Microsoft® Windows 2019	✓
Microsoft® Windows 2022	✓
Red Hat® Enterprise Linux 7	✓
Red Hat® Enterprise Linux 8	✓
Red Hat® Enterprise Linux 9	✓
Oracle Solaris 11	✓

PAM A2A languages	Supported?
Java	✓
C++	✓
C	✓
C#	✓
PHP	✓
Python	✓
JavaScript	✓
Perl	✓
PowerShell	✓
Korn Shell	✓
C Shell	✓

**PAM Socket Filter Agent (SFA)**

Installed on an endpoint, the Socket Filter Agent is used to provide lateral containment (such as preventing administrators from “leap frogging” to another server)

PAM SFA Client	Supported?
IBM AIX 6.1 64-bit	✓
IBM AIX 7.1 64-bit	✓
Debian 6 32-bit	✓
Debian 6 64-bit	✓

PAM SFA Client	Supported?
Debian 7 32-bit	✓
Debian 7 64-bit	✓
HP-UX 11i v3 IA64	✓
Red Hat Enterprise Linux 6 32-bit	✓
Red Hat Enterprise Linux 6 64-bit	✓
Red Hat Enterprise Linux 7 64-bit	✓
Oracle Solaris 10 SPARC 64-bit	✓
Oracle Solaris 11 x86-64 (64-bit)	✓
SUSE Linux Enterprise Server 11 32-bit	✓
SUSE Linux Enterprise Server 11 64-bit	✓
SUSE Linux Enterprise Server 12 64-bit	✓
Microsoft® Windows 2016	✓
Microsoft® Windows 2019	✓
Microsoft® Windows 2022	✓

### Windows Proxy

The Windows Proxy is a Credential Manager component that enables updating Windows-based account passwords, and updating Windows service and scheduled task login account passwords.

PAM Windows Proxy	Supported?
Microsoft® Windows 10	✓
Microsoft® Windows 11	✓
Microsoft® Windows 2016	✓
Microsoft® Windows 2019	✓
Microsoft® Windows 2022	✓

### PAM SC Endpoint Agents

To implement PAM Server Control *host-based security*, install the following PAM SC endpoints, as required:

- **Endpoint Agents:** Install on Windows and UNIX servers that you want to secure with PAM SC.
- **UNAB Authentication Agent:** Install on UNIX servers with an Active Directory data store that you want to act as a single repository for all of your users.

For platform support information for PAM SC Endpoint agents, see the [Privileged Access Manager Server Control Endpoint Compatibility Matrix](#).

## Cryptography

Privileged Access Manager uses the following cryptographic algorithms and protocols:

- **Symmetric Encryption:** Advanced Encryption Standard (AES) Symmetric keys of 256 bit key length, defined in NIST FIPS PUB 197 and ISO/IEC 18033-3.
- **Asymmetric Encryption:** Transport Layer Security protocol follows IETF RFC 5246 version 1.2 (TLS 1.2) including optional Perfect Forward Secrecy Diffie Hellman key exchange elliptic curve (P-256 and P-384 supported).
- **Cryptographically secure entropy source:** For symmetric key generation Intel RDRAND (on PAM hardware or if present in the hypervisor hardware for OVF) which meets NIST SP800 90B.
- **Digital Signature:** Digital Signature Standard (compliant to FIPS 186-4) Elliptic Curve Digital Signature Algorithm (ECDSA) (P-256 and P-384 supported).
- **Hash Functions:** For integrity checks and comparison of User specific login credentials, SHA-2 hash is used either with 512 or 256 bits. In SSH-2 communication, HMAC can support either SHA 256 or 512
- **Digital Certificates:** Either RSA (2048 or 4096 key length) or ECDSA (Curve p-256 or p-384) certificates may be implemented on the PAM server.

## Release Comparison

This table compares the key features in 4.1.7 to those in the most recent active PAM 4.1.x releases:

Key Features	4.1.7	4.1.6	4.1.5	4.1.4	4.1.3
New Windows SSH Password and SSH Key Target Connectors	yes	no	no	no	no
PAM UI Dark Mode	yes	no	no	no	no
New External API methods for <a href="#">managing Credential Manager credential groups</a> and <a href="#">obtaining Credential Manager roles</a>	yes	no	no	no	no
PAM Client Control-F Search Support	yes	no	no	no	no
<a href="#">Send Cluster Status and Network Storage emails with TLS</a>	yes	no	no	no	no
<a href="#">System</a> and <a href="#">Cluster</a> Dashboards	yes	yes	no	no	no
<a href="#">LDAP Synchronization Scheduling</a>	yes	yes	no	no	no
<a href="#">Restrict API Key Role Group Inheritance for External API Users</a>	yes	yes	no	no	no
<a href="#">REST API Support for ServiceNow Integration</a>	yes	yes	no	no	no
<a href="#">Support for Azure SQL Managed Instance User Accounts</a>	yes	yes	yes	no	no
<a href="#">Just in Time (JIT) Provisioning for Azure SQL Managed Instance User Accounts</a>	yes	yes	yes	no	no
<a href="#">Active Directory</a> and <a href="#">Windows Remote</a> Target Connectors Now Support Kerberos Authentication	yes	yes	yes	no	no
<a href="#">Set Allowed TLS Communication Version</a>	yes	yes	yes	no	no
<a href="#">Changes to Oracle Target Connector Logic When Updating Target Accounts</a>	yes	yes	yes	no	no
<a href="#">JSON Message Format Option Added for Syslog and Splunk Server Logging</a>	yes	yes	yes	no	no
<a href="#">IPv6 Addressing Support</a>	yes	yes	yes	yes	no
<a href="#">Display a message to users at login</a>	yes	yes	yes	yes	yes
<a href="#">A2A Client for Red Hat Enterprise Linux Now Available As an RPM Package</a>	yes	yes	yes	yes	yes
<a href="#">Route OCSP Requests Through an OCSP Proxy Server</a>	yes	yes	yes	yes	yes
<a href="#">New option to hide "View Credential" link from users accessing a TCP/UDP service from the Access panel</a>	yes	yes	yes	yes	yes
<a href="#">Updated SPFD (Service Provider Daemon) logging</a>	yes	yes	yes	yes	yes

Key Features	4.1.7	4.1.6	4.1.5	4.1.4	4.1.3
PAM Client Supports ARM64 Architecture	yes	yes	yes	yes	yes
Support for AWS EC2 instances in the GovCloud Eastern Region (US-Gov-East) as well as eu-south-1 (Milan), eu-central-2 (Zurich), and eu-south-2 (Spain) in commercial cloud	yes	yes	yes	yes	yes
Number of Credential Manager groups that can be assigned to a user is no longer limited	yes	yes	yes	yes	yes
Admins can now see all target account information when scheduling a database back up	yes	yes	yes	yes	yes
Cluster key now cleared after a node leaves the cluster	yes	yes	yes	yes	yes

**NOTE**

For information about features in earlier 4.1.x releases, see the [4.1.2 Release Comparison](#).

## New Features in 4.1.7

This topic introduces the following new features and enhancements in PAM 4.1.7.

### Windows SSH Password and SSH Key Target Connectors

This release provides two new SSH-based target connectors that provide secure solutions for managing local privileged credentials on supported SSH-enabled Windows systems:

- **Windows SSH Key target connector**
- **Windows SSH Password target connector**

**NOTE**

The Windows SSH Key target connector is the most secure. Both new connectors are more secure than the Windows Remote target connector.

For more information, see:

- [Windows SSH Key Connector](#)
- [Windows SSH Password Connector](#)

### PAM UI Dark Mode

This release introduces an application color scheme setting that allows you to configure the PAM UI to be displayed using a new **Dark** mode instead of the existing **Light** mode (which is still the default). The application color scheme is configured as a **Global** setting, but can be overridden by local account settings after a user logs in.

**NOTE**

Dark mode is also not available on the PAM Agent or for all locations on other PAM UI platforms, including the following elements and components:

- PAM access methods (for example, RDP, SSH, and TELNET) launched from the **Access** page
- PAM LDAP Browser
- Session Recording Viewer
- Threat Analytics
- PAM Report output
- External API Documentation
- Online help
- Alternate Configuration Utility



For more information, see [Configure Global Settings](#) and [Configure Your Account Settings](#).

### **New External API Methods for Managing Credential Manager Credential Groups and Obtaining Credential Manager Roles**

**Managing Credential Manager credential groups:** In previous releases, you could only manage Credential Manager credential groups using the CLI interface. This release adds REST methods that allow you to do the same operations using the External REST API. For more information, see [Get Credential Manager Roles Using the External API](#).

**Obtaining Credential Manager Roles:** In previous releases, you could only get Credential Manager roles using the CLI interface. This release adds a REST method that allows you to get roles using the External REST API. For more information, see [Get Credential Manager Roles Using the External API](#).

### **PAM Client Control-F Search Support**

Previously, you could use the industry-standard Control-F keyboard shortcut to search PAM browser-based pages when accessing the PAM UI from a browser but not from the PAM Client. Examples of searchable pages include PAM reports, the Web Portal, the SAML IdP login page, and the Threat Analytics Console.

This release adds the same search functionality to the PAM Client. That is, when using the PAM client you can now use the Control-F keyboard shortcut to search the same pages as you can when accessing the PAM UI from a browser.

### **Support for Sending Cluster Status and Network Storage Emails Over a Secure TLS Connection**

PAM has provided the option to use TLS to secure the connection to the SMTP server configured for Credential Manager-related email messages (on the **Configuration, Email Settings** panel) since release 3.4.5. However, Cluster Status and Network Storage Status emails continued to be sent using the SMTP server configured on the **Configuration, Monitor (Legacy)** panel, which did not support a TLS connection.

In release 4.1.7, PAM uses the SMTP server that is configured to send Credential Manager-related email (which does support TLS) to also send Cluster Status and Network Storage Status emails.

#### **IMPORTANT**

After upgrading to 4.1.7, Cluster Status and Network Storage Status emails will only be sent if PAM is configured to send Credential Manager emails. If not, complete the procedure that is described in [Configure Email Preferences for Password View Policies](#) before or immediately after upgrade.

### ***Credential Manager Email Settings Used for Cluster Status and Network Storage Emails***

PAM uses the following settings from the **Configuration, Email Settings** panel to send Cluster Status and Network Storage emails:

- **Enable SMTP Server Authentication:** An account to use to authenticate with the SMTP server.
- **Hostname:** Identifies the SMTP server.
- **Port:** The port number of the SMTP server.
- **Enable TLS:** If set, secures the connection to the SMTP server using TLS.

### ***Other Configuration Settings Used to send Cluster Status Emails***

PAM uses the following settings that are defined on the **Configuration, Monitor (Legacy)** panel to send Cluster Status emails:

- **Admin Email:** The email address (or addresses) of the user (or list of users) to which Cluster Status emails are sent.
- **Appliance From Address:** An email address that specifies the "From" address of sent Cluster Status emails.

### ***Other Configuration Settings Used for Network Storage Status Emails***

PAM uses the following settings to send Network Storage Status emails:

- **"To" Address:** Network Storage Status emails are sent to the addresses of all users with the Global Administrator or Configuration Manager role.
- **Appliance From Address** (on the **Configuration, Monitor (Legacy)** panel): An email address that specifies the "From" address of sent Network Storage Status emails.

## New Features and Enhancements in Earlier 4.x Releases

The topics in this section describe the features and improvements provided in earlier Privileged Access Manager 4.1.x releases

Use the table of contents to access these topics.

### New Features in 4.1.6

This topic introduces the new features and enhancements in PAM 4.1.6.

#### System and Cluster Dashboards

This release provides the following dashboards for viewing and interpreting data about PAM nodes and clusters:

- **System Dashboard:** Available in the PAM UI, visualizes data about the current PAM instance
- **Cluster Dashboard:** Available in the Management Console, visualizes data about a PAM cluster.

Both dashboards show current and historical data that dynamically updates at specified intervals, making them valuable tools for monitoring performance and identifying trends over time.

For more information, see [System Dashboard \(Single Node\)](#) and [Management Console Cluster Dashboard](#).

#### LDAP Synchronization Scheduling

In this release, you can configure PAM to synchronize with LDAP servers according to a specified schedule. Scheduling allows you to avoid running the update during peak periods when PAM servers are experiencing heavy loads. In environments with multiple LDAP instances, you can also use scheduling to stagger the order and timing of refreshes for each instance. (Previously, you could only configure PAM to synchronize with LDAP servers according to a specified interval.)

For more information, see [How to Set Up LDAP Servers for User Authentication](#). (Look for Step 8 in the "Identify the LDAP Servers in Your Environment" procedure.)

#### Restrict API Key Role Group Inheritance for External API Users

The External REST API uses the role assignments that are defined in API keys associated with user accounts to authorize calls to its methods. By default, each API key has the same role assignments as those configured to determine the privileges of that account to use the PAM UI. The API key can therefore be used to access to the same functionality using the External API as its associated user account using the PAM UI.

In previous releases, you could edit an API Key definition to reduce its privileges to use the External API by removing roles that were *directly assigned* to the user account. However, you could not remove roles *inherited from user groups* of which the user was a member.

In this release you can also remove roles inherited from user groups of which the user is a member.

For more information, see [Deploy the External REST API \(Administrators\)](#).

#### REST API Support for ServiceNow Integration

In this release, you can configure PAM to connect to ServiceNow using the REST API protocol. Previously, the API exclusively used the SOAP web service interface (which is still the default) to connect to ServiceNow.

For more information, see [ServiceNow Integration](#).

## New Features in 4.1.5

This topic introduces the new features and enhancements in PAM 4.1.5.

### **Support for Azure SQL Managed Instance User Accounts**

This release provides a new *MSSQL Azure Managed Instance* application type and target connector that enables Credential Manager to manage accounts on an Azure SQL Managed Instance.

For more information, see [Add an MSSQL Azure Managed Instance Target Connector](#).

### **Just in Time (JIT) Provisioning for Azure SQL Managed Instance User Accounts**

This release provides *Just in Time (JIT)* provisioning, which allows you to dynamically provision and deprovision Azure SQL Managed Instance user accounts on demand.

JIT provisioning provides the following security enhancements for accessing your Azure SQL Managed Instance:

- Zero-trust security where user identities only exist on the Azure SQL Managed Instance during the checkout period.
- On-demand identity and access management with dynamic privileges that is auditable and can be subject to third-party approval.

For more information, see [Configure Just in Time \(JIT\) Provisioning for Azure SQL Managed Instance User Accounts](#).

### **Active Directory and Windows Remote Target Connectors Now Support Kerberos Authentication**

In this release, the Active Directory and Windows Remote target connectors have been updated to support Kerberos authentication.

For more information, see [Add an Active Directory Target Connector](#) and [Add a Windows Remote Target Connector](#).

### **Set Allowed TLS Communication Version**

In this release, you can use the **TLS Communication Allowed** feature to select the TLS communication version to use with a Utility Group:

- Selecting the **All Versions** option means that PAM uses your current TLS settings with a Utility Group.
- The **TLS V1.2** option means that PAM only uses TLS version 1.2 with a Utility Group.

For more information, see the section entitled [Step 6. Enable the TLS Settings](#), in the [Enabling Server Control TLS Settings](#) topic.

### **JSON Message Format Option Added for Syslog and Splunk Server Logging**

In this release, you can configure PAM to send log messages to Syslog and Splunk servers using the JSON message format. Previous releases supported XML and Space Delimited formats

For more information, see [Configure a Remote Syslog Server](#), [Configure a Splunk Server for Logging](#), and [Syslog Message Formats](#) (which contains JSON-formatted examples in the "Metric Detail JSON Example" and "Audit Detail JSON Example" sections).

### **Changes to Oracle Target Connector Logic When Updating Target Accounts**

The Oracle target connector credential update workflow has been modified to ensure endpoint Oracle server logs only reflect actual failed login attempts. Previous workflows still tested new, system-generated credentials prior to the update, resulting in extraneous errors. This workflow was a holdover from manual password generation. To ensure that

the PAM and endpoint Oracle Server log audit records only reflect actual failed login attempts, the Oracle target connector now does not attempt to log in with a new, system-generated password for an account being actively managed.

### **Functional Change**

#### **NOTE**

**The RSA client is updated in this release, requiring RSA server platform configuration changes!** For more information, see the [Register PAM as an Authenticating Device on the RSA SecureID Authentication Manager Server](#) section of the [Configure the Product for RSA SecurID](#) topic.

## **New Features in 4.1.4**

The PAM 4.1.4 release focuses on one major new feature: *IPv6 addressing support* and provides *one functional change*.

### **IPv6 Addressing Support**

This release updates PAM to support IPv6 addressing so that it can operate in an IPv6 environment.

#### **NOTE**

All PAM components have been updated to support IPv6 addresses with the following exceptions, which remain IPv4-only in this release:

- PAM SC Utility Appliances
- PAM SC endpoints
- Sybase target connectors

### **IPv6 Addressing Functional Examples**

The following list shows some functional examples of the use of IPv6 addressing in a PAM environment:

- Administrators can now use IPv6 addresses when configuring the PAM cluster. For more information, see [Configure a Cluster](#).
- Administrators can download the PAM installation software from an IPv6 address. For more information, see [Deploy the PAM Client](#).
- Users can now log in to the PAM Client using an IPv6 address. For more information, see [Privileged Access Manager Client Reference](#).

### **Key IPv6 Addressing Configuration Settings**

The following entries show some of the most significant configuration settings that are required to enable and use IPv6 addressing:

- *Enable PAM IPv6 addressing*, configure a default IPv6 gateway, and configure IPv6-compatible network Interfaces on the **Configuration, Network, Network Settings** panel. For more information, see [Configure Network Settings](#).
- Configure IPv6 addresses when configuring the PAM cluster. For more information, see [Configure a Cluster](#).

### **Functional Change**

In this release, the **Docker Network Settings** panel has been renamed to **Container Network Settings** and the controls on it are changed. For more information, see [Configure Container Network Settings](#).

#### **NOTE**

There are also some changed and new External API calls related to the container network changes. For more information, see [New and Revised External API Calls in 4.x and 4.x.x Releases](#).

## New Features and Enhancements in 4.1.3

This topic introduces the new features and enhancements in PAM 4.1.3.

This release includes the following new features:

- [Display a Message to Users at Login](#)
- [A2A Client for Red Hat Enterprise Linux Now Available As an RPM Package](#)
- [Route OCSP Requests Through a Proxy Server](#)
- [New Option to Hide "View Credential" Link From Users Accessing a TCP/UDP Service from the Access Panel](#)

### NOTE

For the list of enhancements, see [New Functional Enhancements](#).

### Display a Message to Users at Login

In this release, you can configure a message that appears when a user logs in to the PAM UI. Examples of the types of notifications you might want to present in these messages include the following items:

- Planned maintenance
- Availability of training for new available features
- Process changes

For more information, see [Display a Message to Users at Login](#).

### A2A Client for Red Hat Enterprise Linux Now Available As an RPM Package

This release adds an RPM package for Red Hat A2A Clients. Using this package with a Red Hat native package manager (YUM or DNF) to install the client provides the following benefits:

- To support the efficient installation of the A2A Client on multiple request servers, you can place the RPM package in a central repository of a package handler rather than download it to each host.
- Package handlers can identify from the RPM that the A2A Client requires the **libidn** library and can resolve this dependency by installing the correct version automatically, if necessary. (You have to do these actions manually when using the standard UNIX install script.)
- Package handlers can identify an existing A2A Client that was installed from an RPM package and can upgrade it automatically. (A2A Clients that were installed using the UNIX install script do not support upgrades.)

For more information, see [Install and Activate an A2A Client on a Request Server](#).

### Route OCSP Requests Through a Proxy Server

This release allows you to configure a proxy server to allow requests and responses through the firewall.

For more information, see [Route OCSP Requests Through a Proxy Server](#).

### New Option to Hide "View Credential" Link From Users Accessing a TCP/UDP Service from the Access Panel

In previous releases, when a TCP/UDP Service was configured with **Application Protocol** set to **Disabled**, a **View Credential** link was displayed when a user selected the corresponding service icon on the **Access** panel:

In this release, you can set the new **Hide Credential** configuration setting configuring a TCP/UDP service to hide the **View Credential** link.

For more information, see [Create TCP/UDP Services to Access a Device](#).

### **New Functional Enhancements**

This release adds support for the following functional changes:

- [Support for Additional AWS Regions Enabled](#)
- [Admins Can Now See All Target Account Information When Scheduling a Database Backup](#)
- [Updated SPFD \(Secure Port Forwarding Daemon\) Logging](#)
- [Number Of Credential Manager Groups That Can Be Assigned To A User Is No Longer Limited](#)
- [Cluster Key Now Cleared After a Node Leaves the Cluster](#)
- [PAM Client Supports ARM64 Architecture](#)

### **Support for Additional AWS Regions Enabled**

This release adds support for AWS instances for three new European regions: eu-south-1 (Milan), eu-central-2 (Zurich), and eu-south-2 (Spain), as well as the GovCloud Eastern region (US-Gov-East).

For information, see [Configure Privileged Access Manager for AWS](#).

### **Admins Can Now See All Target Account Information When Scheduling a Database Backup**

PAM administrators, can now see all target account information when you schedule a database backup. Target account information includes the target account name, device, type, and target account device name. Also, the UI now shows the device that is associated with the account.

Previously, the administrator could only see the target account name when scheduling a database backup, and not this additional information. If two or more accounts had the same name, it was impossible to determine the correct account because you were unable to see any supporting account information.

For more information, see the [Schedule a Backup of the Database](#).

### **Updated SPFD (Secure Port Forwarding Daemon) Logging**

To configure WolfSSL logging levels, use the **SPFD Log Level** on the **Configuration, Diagnostic Logs** panel, which now includes revised and new options.

For more information, see [Configure and Obtain Diagnostic Logs](#).

### **Number Of Credential Manager Groups That Can Be Assigned To A User Is No Longer Limited**

In prior releases, by default you could assign only 10 Credential Manager groups to a user. (Although this limit could be increased to 25 using a procedure provided by Broadcom Support). In this release, there is no limit to the number of groups that you can assign regardless of whether you were previously using the default or expanded limit.

### **Cluster Key Now Cleared After a Node Leaves the Cluster**

In earlier releases, the cluster key was retained in the configuration information of a node after that node had left the cluster, had been ejected from the cluster, or the cluster was reset. In this release, the key is cleared when a node leaves the cluster for any reason.

### **PAM Client Supports ARM64 Architecture**

In this release, the PAM Client adds native support for Apple ARM64 architecture. Installation packages for both MacOS Intel and MacOS ARM64 platforms are now available for download and deployment. Existing PAM Clients for MacOS will continue to use Intel binaries when they self-update to 4.1.3. A fresh install of PAM Client is required to deploy ARM64 binaries.

## **New Features and Enhancements in 4.1.2**

This topic introduces the new features and enhancements in PAM 4.1.2.

### **Updated Cryptographic Providers**

This release provides the following cryptographic provider updates:

- For servers running in FIPS mode, the WolfSSL module has been updated to a version that incorporates the FIPS 140-2 validated FIPS Object Module (FOM) under CMVP Certificate #3389.
- For servers not running in FIPS mode, OpenSSL has been replaced with WolfSSL but does not use the validated FOM. This change does not affect established Key-Encryption-Key or Server Key (Data-Encryption-Key) currently in use.

### **Support for the ed25519 Cryptographic Algorithm**

This release supports the ed25519 cryptographic algorithm for more secure SSH communications during **credential management** and **access management**.

#### ***Credential Management***

For credential management, Cisco and UNIX target connectors can now use the following new, more-secure cryptographic algorithms in non-FIPS mode:

- Key Exchange algorithm: curve25519-sha256,curve25519-sha256@libssh.org
- Server Host Key: ssh-ed25519

For more information about this and other supported security algorithms for credential management using Cisco and UNIX target connectors, see the [Review Strong Cryptography on Cisco and UNIX Target Connectors](#) section of the [Upgrade Prerequisites for 4.1.2](#) topic.

#### **NOTE**

Prior to upgrading to **4.1.2**, if the **Use supported algorithm** checkbox option was selected for all the algorithms under the SSH-2 tab, this checkbox continues to stay selected, or will get cleared (that is, unchecked), depending on the version of PAM from that you are upgrading.



Upgrading from **4.1 to 4.1.2** preserves the **Use supported algorithm** checkbox option. This upgrade path also adds the newly Key exchange algorithm curve25519-sha256, curve25519-sha256@libssh.org, and Server Host Key ssh-ed25519 to the default list as high priority algorithms, and connectors continue working using the recommended list. No user action is required.

Upgrading from **4.0.x to 4.1.2** will NOT preserve the **Use supported algorithm** checkbox option: this check becomes cleared (that is, unchecked). Review the algorithms for every application, and either provide a customized list, or select the **Use supported algorithm** checkbox option, and let the connectors use the recommended list. This upgrade path uses the new Key exchange algorithm curve25519-sha256, curve25519-sha256@libssh.org, and Server Host Key ssh-ed25519 as high priority algorithms set by the recommended list. User action is required.

## Access Management

For access management, ed25519 cryptographic algorithm is now one of the preferred cryptographic algorithms to help secure SSH communications using SSH Proxy and SSH Mindterm. In addition to supporting the ed25519 cryptographic algorithm, the following algorithm changes were made to SSH Proxy and SSH Mindterm:

### SSH Proxy

- Added to the PAM recommended list of Key Exchange for non-FIPS mode only: curve25519-sha256
- Server Host Keys algorithms added to the PAM recommended list of Server Host Keys for non-FIPS mode only: ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
- Server Host Keys algorithms added to the PAM recommended list of Server Host Keys for FIPS Mode: ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
- *Unsupported* Server Host Keys: ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com

#### NOTE

If an existing cryptographic configuration for SSH Proxy is configured to use one of the unsupported algorithms, remove them using the PAM UI, and then save the configuration settings. If the unsupported algorithms are not removed from the customized Server Host Key list, the PAM UI will not allow any updates to be done to SSH Proxy cryptography algorithms.

### SSH MindTerm

Key Exchange:

- Added to the PAM recommended list for non-FIPS mode only: curve25519-sha256,diffie-hellman-group14-sha256
- Added to the PAM recommended list for FIPS Mode: diffie-hellman-group14-sha256
- Added to the PAM supported list for non-FIPS mode: curve25519-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512
- Added to PAM supported list for FIPS mode: diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512

Server Host Key:

*Added* to the PAM recommended list for both FIPS and non-FIPS mode: ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521

#### NOTE

If the **Use default** option was selected on either the **SSH-Proxy** and/or the **SSH Mindterm** tabs, after upgrade to 4.1.2, this option becomes cleared (that is, unchecked) due to a change in the recommended algorithm. Select the **Use default** option, and continue using the updated PAM recommended list. You can also customize the algorithm selection.



For more information about this and other supported and recommended lists of the security algorithms for access management, see the [Review Strong Cryptography for Access Management - SSH Proxy and SSH Mindterm](#) section of the [Upgrade Prerequisites for 4.1.2](#) topic.

### **PAM Client Supports Apple macOS Ventura**

In this release, the PAM Client adds support for Apple macOS Ventura.

### **Web Proxy Support**

This release adds the ability to configure *web proxy definitions* to represent physical (or virtual) web proxies in your network. Use web proxy definitions when configuring [services to access web portals](#) if the network firewall would block a direct connection to the portal.

For more information, see [Configure Web Proxy Definitions](#).

#### **NOTE**

This feature was originally implemented in the 4.0.4 release.

### **Access Panel Improvements**

#### **NOTE**

In this release, the title of the list of devices on the **Access** panel is changed to **Access Devices**.

In previous releases, you could only use the **Access** panel when logged into the PAM UI from a PAM client, PAM Agent, or Internet Explorer.

In this release, a *limited* version of the **Access Devices** panel available when logged in to the PAM UI from a standard browser (for example, Chrome, Edge, Firefox, or Safari) allows you to do the following tasks:

- Obtain the credentials of any target account (of a target application maintained on a Privileged Access Manager device) for which you have privileges in the **Access Devices** table.
- View the details of any credentials that you are using in the **Passwords currently in use** table.

For more information, see [Use the Limited Functionality Access Devices Panel on Standard Web Browsers](#).

#### **NOTE**

This feature was originally implemented in the 4.0.4 release.

### **Improved Session Recording Reconciliation**

PAM runs the following *session recording reconciliation processes* that identify session recordings that do not have a corresponding metadata file or database entry. If a discrepancy is found, the reconciliation processes reconcile that discrepancy by creating the missing element:

- **Most Recent Recordings:** Reconciles recent (up to three days old) session recordings. Runs hourly.
- **All Other Recordings:** Reconciles other session recordings. Runs daily.
- **Restored Recordings:** Reconciles session recordings [recovered from archives](#). Runs hourly.

For more information, see [Configure and Manage Session Recording](#).

The **System Activity** tab on the **System Info** pane provides detailed information about the status of each reconciliation process. For more information, see [View System Information](#).

#### **NOTE**

This feature was originally implemented in the 4.0.4 release.

### **Session Recording Storage Configuration Security Enhancement**

Previously, when a CIFS share was configured as the session recording external storage provider, the PAM UI showed the password of the CIFS administrator in clear text. In this release, the CIFS administrator password is obscured.

#### **NOTE**

To configure external storage for session recording, navigate to the **Configuration, Logs, Session Recording** panel and select the **External Storage** tab.

#### **NOTE**

This feature was originally implemented in the 4.0.4 release.

### **Remote Storage Session Recording Performance Improvement**

To mitigate performance issues initiating session recordings on remote storage, PAM now writes the session recordings for each day in a correspondingly named subdirectory ( *YYYYMMDDPAM* ). This change in infrastructure is transparent to session viewers; the physical location of files is not shown on the **View Session Recordings** panel.

#### **NOTE**

This feature was originally implemented in the 4.0.4 release.

## **New Features and Enhancements in 4.1.1**

This topic introduces the new features and enhancements in PAM 4.1.1.

### **PIV Authentication and Authorization Activity Now Included for Management Console**

In this release, the Management Console supports The following PIV authentication and authorization functionality:

- **Authorized users can access the Management Console UI using PIV Authentication:** Authorized users can access the Management Console UI using PIV Authentication.
- **Authorized Admins can approve PIV-users from the Management Console:** Admins can now also approve all PIV logins from either the Management Console web-UI or the standard PAM web-UI.

Access the following topic links to learn how you can now use the [Management Console](#) to [approve Smart Card users logins](#), and [configure Active Directory for user authentication](#).

### **Just in Time (JIT) Provisioning for MSSQL User Accounts**

This release provides *Just in Time (JIT)* provisioning, which allows you to dynamically provision and deprovision Microsoft SQL Server (MSSQL) user accounts on demand.

JIT provisioning provides the following security enhancements for accessing your SQL Server database:

- Zero-trust security where user identities only exist on SQL Server during the checkout period.
- On-demand identity and access management with dynamic privileges that is auditable and can be subject to third-party approval.

For more information, see [Configure Just in Time \(JIT\) Provisioning for MSSQL User Accounts](#).

### **Extended Timeout Functionality Allows Long Jobs to Run Unattended Without Timing Out**

In this release, a new *Extended Timeout* option allows users who must run lengthy jobs (such as database backups) to specify a value longer than the global **Connection Idle Timeout** (formerly named **Applet Timeout**) value. When **Extended Timeout** is enabled in an associated access policy, users are prompted to optionally specify a longer idle timeout (up to the new global **Maximum Connection Idle Timeout** setting) when starting an access session. For more information, see [Set Up a Policy](#).

## **Improved PAM SC Device Matching**

PAM can automatically match Server Control devices. However, if a match fails, PAM defaults to creating a device. With this release, the match process is more accurate, and you now have more control over the match criteria. Even if the match does not succeed and PAM creates a device, you can still edit the Name and Address fields of the device. For more information, see [Associating PAM SC Devices with PAM Devices](#).

## **Configure the CIDR Docker Network Settings**

As a PAM Administrator, you can edit the CIDR used by Docker in PAM. For more information, see [Configure Docker Network Settings](#).

## **Enable or Disable TLS Ciphers**

The Super, Global Admin, or Configuration administrators can now disable or enable cipher suites that are used by the PAM Cryptography security settings. For more information, see the **Enable or Disable TLS Cipher Options** section of the [Configure SSH Proxy, SSH MindTerm, and TLS Cryptography Options](#) topic.

## **Enabling Server Control TLS Settings**

As an administrator, you can use the **TLS Settings** screen to specify your own root certificate, a corresponding public key certificate, a corresponding private key, and an optional passphrase for the private key as **Secrets**. After configuring the **TLS Settings**, you can assign them to Utility Groups. OnePAM then distributes the configured root certificate and the public and private keys to individual Utility Groups whenever the pam-dh service on a Utility Appliance restarts. For more information, see [Enabling Server Control TLS Settings](#).

## **Remote Storage Session Recording Performance Improvement**

To mitigate performance issues initiating session recordings on remote storage, PAM now writes the session recordings for each day in a correspondingly named subdirectory (`YYYYMMDDPAM`). This change in infrastructure is transparent to session viewers; the physical location of files is not shown on the **View Session Recordings** panel.

## **Full Backup Of Hardware Appliances When Applying Hotfixes That Require A Reboot is Now Optional**

When applying a hotfix *that requires a reboot* to a 4.1.1 (or later) PAM hardware appliance, full backup of the appliance is now optional.

# **New Features and Enhancements in 4.1**

This topic introduces the new features and enhancements in PAM 4.1.

## **Secrets Management**

Secrets management is access control for human users and programs to sensitive and privileged information. That information might include X509 certificates, connection strings, tokens, configuration parameters, encryption keys, credentials, and so on.

PAM Secrets Management lets you control access to any information that your organization regards as secret, wants to protect, and wants to provide fine grained, auditable authorization. That information might include X509 certificates, connection strings, tokens, configuration parameters, encryption keys, credentials, and so on. PAM gives Security Teams the ability to store, audit, and securely share this information with authorized recipients: people or processes.

For more information about Secrets Management, see [Secrets Management Overview](#).

---

### **Clusters Now Support External Load Balancers to Handle Site Traffic**

Previously, PAM only offered an internal load-balancing solution in which requests addressed to a site VIP were redirected by the site leader to the least-loaded site member using a software-based load-balancing algorithm. This release supports the use of an external load balancer to redirect requests that are addressed to the site VIP to the least loaded site members using its own load-balancing algorithm.

For more information about using external load-balancing, see [Internal and External Load-Balancing](#)

### **Download Advanced Metrics Files To Assist Broadcom Support Troubleshoot Your Issue**

In this release, you can download *advanced metrics files* that Broadcom Support can import into their own test systems to analyze items that are related to an issue you are encountering.

For more information about downloading advanced metrics files, see [Configure Diagnostic Logs](#).

### **New Option Allows Use of Checksums During Upgrade**

This release provides a new **Show Checksums** option that recomputes the checksum value of a downloaded file to verify that the file was not corrupted during the upload process. Compare this newly generated value with the value of the checksum file included in the downloaded zip file.

For more information, see [Upgrade](#).

### **Troubleshooting Tools for Policies Deployed on Server Control Devices and Device Groups**

This release provides tools that help with troubleshooting policies that are deployed on Server Control Devices and device groups.

For more information, see [Troubleshoot Policies Deployed on Server Control Devices](#) and [Troubleshoot Policies Deployed on Server Control Device Groups](#).

### **Troubleshooting Tools for Policies Deployed on Server Control UNAB Devices and Device Groups**

This release provides tools that help with troubleshooting policies that are deployed on Server Control UNAB devices and device groups.

For more information, see [Troubleshoot Policies Deployed on UNAB Devices](#) and [Troubleshoot Policies Deployed on UNAB Device Groups](#).

### **Utility To Extract PIM Shared Account Management Data When Migrating to PAM**

This release provides a utility that extracts PIM Shared Account Management (SAM) data to enable migration from PIM to PAM.

For more information, see [Extract PIM Shared Account Management \(SAM\) Data](#).

### **Exportable PAM SC Device Agent Status Report**

In this release, you can export a report showing PAM SC Device agent status.

For more information, see [View Server Control Endpoint Agent Status on the Device Agent Status Screen](#).

### **Credentials Obtained for Viewing by Dual Authorization Can Now Be Viewed or Used for Auto Connect**

Previously, if a credential was obtained for viewing by a dual authorization password view request, it could only be viewed, not used for auto-connect. In this release, if a credential is approved for viewing it is also approved for auto-connect. However, it is still the case that if a credential is approved for auto-connect, it can only be viewed by canceling the auto-connect request and submitting a new request for viewing (and that request being approved).

## New Features and Enhancements in 4.0

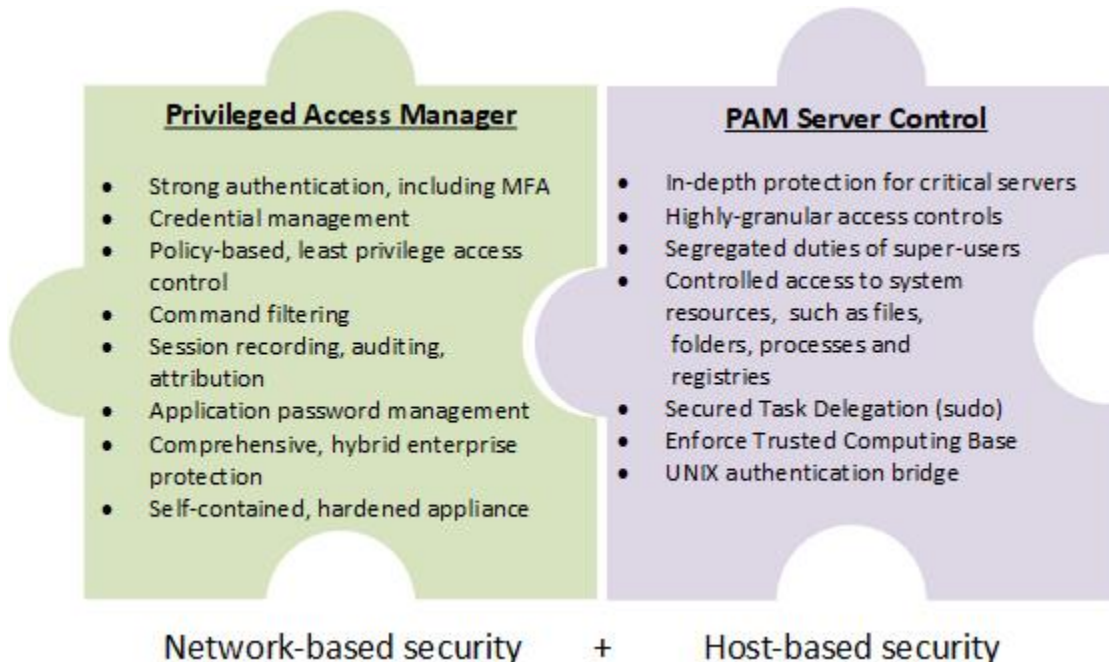
### PAM Server Control Unification

The primary new feature in this release is the *Server Control Module*, which unifies all the capabilities of the standalone *Privileged Identity Manager (PIM)* and *Privileged Access Manager Server Control (PAM SC)* products.

PIM and PAM SC are comprehensive and mature solutions that provide host-based security for your most sensitive systems whether they are physical, virtual, or cloud-based. They provide active, comprehensive security software solution for open systems, tied dynamically to the operating system. Each time a user requests a security-sensitive operation, such as opening a file, substituting a user ID, or obtaining a network service, the product intercepts the event in real time and evaluates the validity of the operation before passing control to the native OS functions.

PIM and PAM SC are highly scalable and provide fine-grained access controls, auditing, and UNIX authentication bridging across servers from a central management console. Server Control is uniquely capable of enforcing access controls on powerful native superuser accounts, like the UNIX and Linux root and Windows administrator.

By unifying the capabilities of PIM and PAM SC in the Server Control Module, PAM adds powerful host-based security to its existing network-based security. This combination of capabilities is shown in the following diagram:



For detailed information about the features and benefits of unifying PAM SC with PAM, see [PAM SC Integration Highlights](#).

### External Directory Authentication and Auto Registration of Privileged Users

This feature provides the ability for PAM to auto-register users at run time both for authentication and authorization without importing the entire user group members. This ensures that the large, and frequently changing Users' group member relationship update does not affect PAM performance or cause a breach in governance rules due to access changes. The authentication is always performed through the External Directory (Groups and User Groups only). See [How to Configure Active Directory for User Authentication](#).

### **Removal of Ambiguity when Multiple Roles are Assigned across Multiple Target Groups**

With this release, the Credential Manager role only applies to the objects scoped by the Credential Manager Target Group in the same Credential Manager Credential Group. Previously, all Credential Manager Roles applied to all Credential Manager Target Groups that the user was a member of.

Security checking has been enhanced around target accounts, passwords, and target applications. Users who have created custom roles need to verify that these roles continue to work in this release. Additional Credential Manager privileges may need to be added to the roles. Also, changes made to fix privilege mixing when a user belongs to multiple credential user groups may also alter a user's access to Credential Management features. See [Delegate Password Management Tasks to Groups](#).

### **Ability to Use SFTP or SCP for File Transfers through SSH Proxy**

You can configure a TCP/UDP SSH Service to do the file transfer operations for a native SFTP or SCP application. Session recording is not activated when either of these features are invoked (the files are not copied into the recording). See [Create an SSH Service to Access a Device](#).

### **Expanded Support for Target Application Creation and Updates Using the External API**

This release adds API support to create and update three Target Application types: Active Directory, Windows Remote, and Windows Proxy. Prior to this release, the ability to create target applications for Windows devices was only available using the CLI interface. The ability to do the same operations using the External REST API means users no longer need to switch between CLI and REST for their automation CRUD operations (\*nix is already available). See [Active Directory Target Connector External API Configuration](#), [Windows Remote Target Connector External API Configuration](#), and [Windows Proxy Target Connector External API Configuration](#).

### **Ability to Use HTML Browser-Only Access to View Credentials on a Secondary Site**

This release unblocks the ability to view credentials and do password approvals from the Credentials, Account screen on the secondary site when using HTML5 compliant browsers. (Prerequisite: remove the Standard User role.) See [How to Set Up a Cluster](#).

### **Ability to Determine the Action for Authenticating a PKI User without Revocation Information**

This release provides the ability to determine if a PKI user should be authenticated when a CRL is invalid or when the CRL and OCSP cannot be reached or are not provisioned in PAM. This option, "When Revocation Information is Unavailable," is enabled when you download CRLs automatically, manually, or when you use OCSP. See [Secure Connections Using SSL Certificates](#).

### **Password View Request Updates**

This Release includes the following updates to the Password View Request feature:

- The Reason Description and Reference Code fields are mandatory when a user attempts to view or access an account which has the Reason Required for View option or the Reason Required for Auto Connect option enabled in the Password View Policy. See [Create a Basic Password View Policy](#).
- A Comments field for a Password View Request is available when the Reason Required for View option or the Reason Required for Auto Connect option is enabled in the Password View Policy. This field is optional, and allows requesters to enter any comments that they want to record with the Password View Request. These comments can be reviewed by an auditor for normal Password View Requests or by the Approver in Dual Authentication or Retrospective Approval workflows. You can also use the Comments field with the [viewAccountPassword](#) CLI command with the new optional Comments parameter.
- A banner is displayed on Password View Requests when the Reason Required for View or Reason Required for Auto-connect option is enabled in the Password View Policy. This banner can contain information about what users need



to enter in the Reason Description and Reference Code fields when they attempt to view a password for an account. You can set this banner on the Credential Manager General Settings page or the Password View Policies page. If set as part of the Password View Policy, it takes priority over the General Setting. See [Create a Basic Password View Policy](#) and [Credential Manager Operation Settings](#). The following CLI commands have been updated or have added parameters that support this feature: [viewAccountPassword](#), [addPasswordViewPolicy](#), [updatePasswordViewPolicy](#), and [setSystemProperty](#).

### **Ability to Update the PAM Host File when Deployed in Restricted High Security Data Centers**

This feature enables users to update the PAM host file from the PAM user interface when doing so through Symantec PAM Support assisted Remote SSH Debug Access is not permitted. See [Custom Host File Entries](#).

### **Enable Public Key Authentication**

You can configure a TCP/UDP Service to connect to a target device using the Public Key Authentication method for a native SSH Application. See [Create an SSH Service to Access a Device](#).

### **Ability to Customize the SSH Cipher Suite Used by PAM for Connections**

PAM provides the ability to configure a subset of ciphers used by SSH connections for accessing devices. The option to configure older vulnerable KEX/Ciphers/HMAC allows the management of legacy devices where newer ciphers are not supported or for systems that have not yet been updated to support the secure default cipher suite of PAM. See [Configure SSH Proxy, SSH MindTerm, and TLS Cryptography Options](#).

### **Keep Alive Sessions**

Support for a configuration option in Symantec Privileged Access Manager (PAM) to enable SSH to save keep alive sessions so that user do not have timeout issues with their sessions. See [Create TCP/UDP Services to Access a Device](#).

### **Web Portal Traffic**

Support for all web portal traffic to be routed through a configured proxy. No user interface changes were made as a result of this feature.

If Symantec ProxySG is configured as a proxy in the PAM client, the following policy configuration change is required on the ProxySG to allow protocols such as SSH and RDP through the ProxySG:

Change:

```
<ssl-intercept>
ssl.forward_proxy (https)
```

To:

```
<ssl-intercept>
ssl.forward_proxy (stunnel)
```

The stunnel configuration allows the ProxySG to intercept other protocols that are tunneled through SSL/TLS, not just HTTPS.

### **The Ability to Run a Network Mapping Job from the PAM Configuration Page**

With the Bulk Network Scan tool, Administrators can run a bulk scan of their network (Host/Port) to determine the status of ports (open/filtered). See [Configure Global Settings](#) and [Networking Tools](#).

### **"Disallow Max Class Repeat" Password Composition Policy**

This password composition policy prevents passwords from containing consecutive characters from the same class. Uppercase, lowercase, numeric, and special characters are the class types.

Example: If MaxClassRepeat is set to 2, then ABcc34^& is allowed, but not AABcc34^&

See [Construct Password Composition Policies](#).

### **Deploy Threat Analytics in Azure**

The PAM Threat Analytics Module, in vhd format, is now supported for deployment in the Microsoft Azure cloud environment. See [Deploy the Symantec Threat Analytics Server](#).

### **New Access Mode in the "Available Credentials" Panel if Credentials are Unavailable**

The "Credential Unavailable" access mode is displayed when credentials are out of sync and have a password view policy with check in/check out or exclusive lock options. The credentials are still presented to the user in the "Available Credentials" panel, but are not actionable.

When a single credential with the access mode "Credential Unavailable" is configured for auto login, a warning popup is displayed and no auto login occurs.

## **Known Issues**

This section describes the currently known issues and workarounds, where available.

### **NOTE**

#### **New Issues in 4.1.7:**

- [SSH Certificate Authentication with an RSA-Based SSH Certificate Authority May Fail with Older Unix/Linux Target Devices](#)
- [Quorum Loss Email Notifications Not Being Sent](#)
- [Local PAM Container Configuration Changes Applied Using the External API Require Server Reboot](#)

### **IPv6 Limitations**

All PAM components support IPv6 addressing with the following exceptions, which remain IPv4-only in this release:

- PAM SC Utility Appliances
- PAM SC endpoints
- Sybase target connectors
- MSSQL Azure Managed Instance target connectors (The Microsoft Azure SQL Managed Instance does not support IPv6 addressing at this time.)

### **Cryptography Issues**

#### ***SSH Certificate Authentication with an RSA-Based SSH Certificate Authority May Fail with Older Unix/Linux Target Devices***

**Symptom:** Configuring PAM with an RSA-based SSH Certificate Authority may fail with older Unix/Linux target devices.

**Workaround:** Some older Unix/Linux variants versions of the sshd server may not support the current default RSA Certificate Signature algorithm: rsa-sha2-512. The previous RSA-based certificate signature algorithm, rsa-sha, was deprecated in 2021 and is no longer considered safe. Try using an ECDSA-based SSH Certificate Authority, or upgrade your sshd server to a more recent version, if possible.

***PKI authentication fails on FIPS-enabled PAM servers when one TLS 1.2 ECDSA cipher is selected (DE545999)***



PKI authentication fails with an "err\_ssl\_client\_auth\_no\_common\_algorithms" error when *one* of the following TLS 1.2 ciphers is enabled for inbound TLS 1.2 traffic:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

#### **NOTE**

There is no issue if you enable both ciphers.

### ***Unsupported Cryptographic Algorithms in Credential Management Workflows***

The following algorithms are not supported in Credential Management workflows.

- Key exchange algorithm: curve25519-sha256
- Server Host Key algorithm: ssh-ed25519

### **Client Issues**

#### ***Cannot Install PAM Client on Mac Silicon Using a Command Line***

**Symptom:** An Admin tries to use a terminal to install the PAM Client on Mac hardware using the following command:

```
sudo ./CAPAMClientInstall.app/Contents/MacOS/CAPAMClientInstall
```

The installation fails and displays the following message:

```
"java" cannot be opened because the developer cannot be verified.
macOS cannot verify that this app is free from malware.
```

**Workaround:** Use Interactive install. After you download the installer file, extract the file, and then run the PAM Client installer.

#### ***Error Message Appears when Launching an RDP Access Method Using PAM Client on a Linux System***

**Symptom:** The following error message appears while launching the RDP Access method using the PAM Client on a Linux system:

```
Unable to load library libpcsclite.so.1 : libpcsclite.so.1 : cannot open shared object: No such file or
directory
```

**Workaround:** To be able to launch the RDP access method, install the **PC/SC Lite smart card** package on a Linux system.

#### ***RDP Client Does Not Support Custom Clipboard Formats (DE532444)***

The RDP Client supports only the following standard clipboard formats for copy and paste operations:

- CF\_TEXT
- CF\_UNICODETEXT
- CF\_DIB

The RDP Client therefore does not support applications that use custom clipboard formats to handle data that cannot be translated into a standard clipboard format. Performing a cut and paste operation in such an application via the RDP client can result in data loss.

**Workaround:** Use the RDP proxy to run applications that use custom clipboard formats.

#### ***User Resource Limit with the A2A Client on an AIX Host***

There is a resource limit when using the A2A Client on UNIX host. The recommended data segment size for user resource limit (ulimit -d) is 1 GB. You have three options.

To **temporarily** increase the data segment size to 1 GB to meet OpenJDK requirements:

**NOTE**

If you do not make a more permanent change as shown in the following options, you must run these commands each time before you start the A2A client

1. Before starting the A2A client, run the following command.

```
ulimit -d 1000000
```

2. Run the following command to start the A2A client (Use your real path if A2A is not installed in /opt/catech):

```
/opt/catech/cspmclient/bin/cspmclntd start
```

To make the data segment size change **permanent for the specified user**, modify the user setting via the AIX chuser command.

**NOTE**

The unit is represented in the number of 512-byte blocks.

```
chuser -d 2000000 root
```

To make a **system-wide change**, edit **/etc/security/limits** to increase the value.

**CA PAM Client Shows an IdP Login Form Instead of an Error Message (DE334815)**

If SAML is not properly configured, the CA PAM Client is displaying a login form. The Client should show the error "An error occurred while processing your request. Please contact your help desk for assistance."

**"Cannot load JVM options" error when launching PAM client on Japanese Windows computer (DE314263)**

Privileged Access Manager does not support installing the CA PAM Client in directories whose names include Japanese characters. If you install the CA PAM Client on a Japanese-language computer, select the Typical option. On the click Install Folder step, enter a folder with no Japanese characters.

**Older Linux installations require more libraries (DE137968)**

This issue occurs when the PAM Client is installed on a workstation that uses older versions of Linux. The PAM Client uses the libXss.so.1 library from libXScrnSaver and the libgconf package. These libraries and packages might not be included in older versions of Linux.

**Workaround:** Ensure libXScrnSaver and libgconf are available on the workstation before you install the PAM Client.

**Credential Management Issues****DeleteTargetAccount CLI Command fails to return expected success response (DE546881)**

The DeleteTargetAccount CLI command successfully deletes the requested target account and returns a status code 400 success message, but does not return expected target account details.

**Account with elevated privileges in Cisco IOS is not supported by Cisco target connector (DE158580)**

An account in Cisco IOS that has Elevated Privileges level 15 is not required to provide credentials when "enable" command is used. That configuration is currently not supported by the Cisco target connector. Such an account cannot be managed by the target application.

**Workaround:** Use another account with privilege level 0 to manage the level 15 account.

**Upgrade Issues****Secondary Backup Drive can cause an upgrade issue (AMI upgrade only)**

If you are upgrading the appliance on an AMI, remove any secondary backup drive that you added for the previous upgrade to 3.0. If you fail to remove the secondary drive, the upgrade completes without producing an error, but your appliance version is not upgraded.

**If Upgrading PAM, then You Must Also Upgrade SFAs**

If you upgrade PAM running in FIPS mode to 4.1.1, then you must also upgrade Socket Filter Agents (SFA) running on Windows target devices to 4.1.1. Until you upgrade Windows SFA devices to 4.1.1, no SFA devices can report violations to PAM instances.

After upgrading a PAM instance running in either FIPS or Non FIPS mode to 4.1.1, you must also upgrade all instances of Windows Socket Filter Agent to 4.1.1 before using ECDSA certificates for inbound TLS connections.

## **Other Issues**

### ***Local PAM Container Configuration Changes Applied Using the External API Require Server Reboot***

You must reboot the PAM server to apply changes that you make to a Local PAM Container using either of the following External API calls:

- `/cspm/ext/rest/config/network/container/local/ipv4`
- `/cspm/ext/rest/config/network/container/local/ipv6`

### ***Quorum Loss Email Notifications Not Being Sent***

Cluster Status notification emails for quorum loss events are not being sent. All other cluster status email are working. The internal defect tracking number for this issue is DE594849.

### ***IPv6 Cluster for PAM Instances Deployed in Azure Cannot Use a Floating IP as the IPv6 VIP Address***

If you want to use an IPv6 cluster for PAM instances deployed in Azure, you cannot use a Floating IP as the IPv6 VIP address. You must use an external load balancer while configuring the IPv6 VIP address. For more information, see *Add Sites to Your Cluster*.

### ***IPv6 Local Loopback Address for RDP Proxy TCP/UDP Services is Not Compatible with Socket Filtering***

A policy using socket filtering that allows access to an RDP Proxy service will have its local IP address for the RDP Proxy Service overridden when the end-user invokes the service. All RDP Proxy instances using socket filtering on an individual user's desktop will then bind to the same local loopback IPv4 address.

If the RDP Proxy TCP/UDP Service defines an IPv6 local IP address ("::1"), then invoking that service in the PAM Client results in the specified IPv6 address being overridden with an IPv4 address.

**Workaround:** An RDP Proxy TCP/UDP Service with a configured client application designed to expect an IPv6 local IP address (<Local IP> surrounded with square brackets) must be modified to expect an IPv4 local IP address (<Local IP> with no square brackets) when socket filtering is in use.

### ***RDP Proxy Does Not Enforce the Connection Idle Timeout Global Setting***

The RDP Proxy does not enforce the **Connection idle Timeout** (formerly **Applet Timeout**) global setting, which is intended to specify the number of minutes of inactivity before a connection with an external device times out.

### ***Selecting Both the "Reason Required for View" and "Reason Required for AutoConnect" PVP Options Generates Duplicate Reports (DE504579)***

Selecting both the **Reason Required for View** and **Reason Required for AutoConnect** PVP options for an application triggers duplicate events that appear twice in the **View Password Requests** report.

**Workaround:** None.

### ***SAML SSO Newly-Configured in 4.1 Does Not Work with an External Load Balancer Address (DE531855)***

Existing configurations that use SAML SSO with external load balancers should continue to work. However, using SAML SSO directly with an external load balancer in the new, more-tightly integrated option in 4.1, does not presently work.

**When configuring SAML connections, the SAML Test button only works for SSL/TLS certificates signed by a Certificate Authority**

Previously, when configuring an Azure connection or PAM as the Service Provider (SP), the SAML **Test** button would work if the IDP had a self-signed or Certificate Authority-signed SSL or TLS certificate. In this release, a security improvement prevents the button from working for self-signed certificates.

#### ***Start of deprecation of the sftpsftp service***

PAM supports file transfers using SSH. As a result, the sftpsftp service is being deprecated over time, in favor of SSH. For this release, sftpsftp service continues to work as expected. However, some sftpsftp error messages are not localized and display only in English.

#### ***Windows 2016 and Windows 2019 not recognized in Device Discovery (DE346437, DE475642)***

Device Discovery does not reliably discover Windows 2016 or Windows 2019. You can set the Default OS to either Windows 2016 or Windows 2019, or manually change the OS after discovery.

#### ***SFA with blacklist throws "Access Denied" message for non-blacklisted IP when launching SSH Proxy service (DE281461)***

An SSH Proxy connection is not terminated in the following circumstances. A Socket Filter Agent with a Blacklist and an SSH Proxy is added to the same device. The Blacklist is configured with the action "Logout of terminal device." A user selects "Restart Session" on the Access page, then selects the SSH Proxy service, and auto-login. The user enters "ssh DeviceIP" of a device that is not blacklisted. An "Access denied" message appears. The connection should be established, but is not.

#### ***Keyboard Mapping Issues (DE158692)***

When using a Linux or Mac OS client, keyboard mapping of some keys for languages other than English would not work correctly for some keyboards.

#### ***Unable to log in to Privileged Access Manager using RADIUS when Two RADIUS Servers are configured (DE172566)***

Redundant RADIUS servers sometimes fail for CHAP authentication when used with One Time Passwords (OTP). This problem causes login failures.

**Workaround:** In the UI, configure the RADIUS server responsible for OTP as the last server in the list of configured RADIUS servers.

#### ***Wrong OS name appears after installing up Windows Proxy***

The user installed a Windows Proxy on a server (such as Windows Server 2016). However, the wrong OS Name appears when the user looks at Credentials -> Manage Targets -> Proxies -> Update -> Type Info

This conflict occurs because the user added an environment variable called JAVA\_TOOL\_OPTIONS, with a value different from the OS name. For example, the user entered JAVA\_TOOL\_OPTIONS: "-Dos.name=Windows 7".

The value specified in the JAVA\_TOOL\_OPTIONS is taking priority showing the OS name instead of actual OS name.

**Workaround:** Because the user customized the OS, the user has to remove the environment variable to view the actual OS in the proxies screen.

#### ***The OS Type and Version Occasionally Improperly Defined During Device Discovery (DE563059)***

PAM Device Discovery uses network scanning along with a set of heuristic rules to identify the operating system (OS) versions for remote systems. However, the results might not be exact, as these results depend on the end user's specific remote servers and network configurations. For example, the OS of a well-hardened server might be more difficult to correctly recognize than a wide-open endpoint OS installation.

**Workaround:** You must confirm these results, which may require manually adjusting the OS versions in the administrative UI.

#### ***Windows AWS instances are incorrectly listed as "Windows 2008" systems on the Devices page (DE492599)***

When Windows AWS devices, for example Windows 2016 Server or Windows 2019 Server, are imported as devices, the associated Operating System entry is incorrectly stated as "Windows 2008" on the **Devices** page.

***Displaying the AWS Access Key Alias, using the Use Alias option, is not Supported in All Sections of the UI and Reports***

On the **AWS Settings** tab, selecting the **Use Alias** option displays the more user-friendly value in the User interface (UI) for the AWS-generated **Access Key ID**. However, the **Access Key Alias** field value may not be available in all sections of the UI. In these sections, the Access Key ID appears instead of Access Key Alias.

## Resolved Issues in 4.1.7

The following table lists the issues that are resolved in release 4.1.7:

Case Number	Internal Defect ID	Resolved Issue
33308508	DE554754	A2A takes interpreter name instead of script name when running Python2 or Python3 scripts.
33401497	DE563110	Primary master failing to start, freezing at "PAM server is starting up."
33404824	DE563495	Vaults are not decrypting Secrets
33529972	DE578466	Delete Key in UNIX SSH applet incorrectly sends a backspace command.
33545614	DE578602	Connecting to a target server via RDP incorrectly displays a popup window which must be clicked multiple times to dismiss.
33571101	DE584927	Some Microsoft Entra ID pages do not load, preventing the use of PAM to manage Entra ID identities
33577016	DE582738	On certain machines, using an A2A script fails to get the hash from the PAM UI or the CLI.
33579613	DE583479	Mac users Cannot Copy/Paste in GitLab Web Portal.
	DE562323	Some keys on non-US keyboards not working when using PAM to access the vSphere Web Portal.
33581135	DE583025	PAM UI sessions experiencing poor performance accessing primary site nodes, with the mysql-slow.log file filling up with the same slow query against the event table on the site and replication leader.
33582305	DE585746	Policy import progress bar stuck at 0% even though policies are imported.
33584316 / 33626804	DE583267 / DE588273	Failover check for authentication using UPN fails during password rotation.
33582259	DE582719	Potential Apache ActiveMQ vulnerability.
33587675	DE586403	Active Directory synchronization is not updating the Target Device OS version.
33588631	DE583599	Database backup scheduler gets stuck trying to send a file to old target server.
33592412	DE583645	RADIUS reauthentication prompt does not work when accessing the PAM UI from a browser.
33594351	DE584380	PVRs created by a user account that no longer exists are not expiring or getting deleted.
33598560	DE585110	Session recordings initiated for PuTTY SSH services that are terminated withing seconds get stuck in status "Recording in Progress."
33600566	DE585218	RDP Proxy failed to connect to target Windows machines after TLS renegotiation strict mode is set.
33600570	DE585086	PAM client user session never times out due to inactivity if you filter on a column on the <b>Credentials</b> , <b>Manage Targets</b> , <b>Accounts</b> page and stay there.
33604447	DE585489	RDP session recordings with size 1K and the status "Encoding Error" cannot be viewed.

Case Number	Internal Defect ID	Resolved Issue
33607589	DE585851	Reason Required text has length constraints.
33612778	DE586647	Radius authentication fails when there is a ' [ ' or ' ] ' in the secret.
33642044	DE589954	Potential cross-site scripting vulnerability detected on the <a href="https://pam_server_ip_or_name/cspm/app/feature/app.html?feature=StandAloneConfig">https://pam_server_ip_or_name/cspm/app/feature/app.html?feature=StandAloneConfig</a> page in the PAM UI.
33642247	DE589966	AIX auto-login fails after password update.
33626476	DE587975	PAM not prompting users logging in using RSA SecurID authentication for a required OTP or dual authentication code.
33631825	DE588930	Password change rollback on anchor server does not complete when using compound servers.
33649470	DE591024	Session recording share outages on some cluster nodes.
33649787	DE591016	Conflict when using special characters on RDP box.
33652430	DE592503	LDAP servers are not synchronizing according to the specified schedule.
33654724	DE591544	DB Backup CIFS Mount failure after updating windows password.
33655152	DE593239	Scheduled LDAP synchronization fails with incorrect "Failed due to the cluster state" message.
33656873	DE591690	searchAuthorization CLI fails with Requestserver.id above int value.
33663788	DE592421	In <b>Global Settings, Maximum Password Length</b> can be set to any value.
33667416	DE593038	TCP/UPD services configured to do WinSCP or FileZilla file transfer operations fail if the connection ID password contains an "@" character followed by a "/" character, with or without other characters between them.
33668509	DE593047	DNs that include a comma in the common name that are copied from Active Directory do not paste correctly into PAM and the resulting DN is not valid.
33674760	DE593939	Unusual high disk utilization errors on all primary cluster nodes.
33023767 / 33412626	DE529787 / DE538447	TA2A clients are not notified about password updates in real time.
33596265 / 33573053	DE584388 / DE565112 / DE583391	Session recording for a specific user results in an Encoding Error and remains unviewable.

## Resolved Issues in Earlier 4.x Releases

The topics in this section describe the issues resolved in earlier 4.x releases,

**Use the table of contents to access these topics.**

### Resolved Issues in 4.1.6

The following table lists the issues that are resolved in Release 4.1.6:

Case Number	Internal Defect ID	Resolved Issue
33397585	DE565344	Post upgrade to 4.1.1, customer encounters sporadic "PAM-CM-0539: A database error occurred" messages.
33437583	DE566771	Non-empty Credential Management groups can be deleted.
33453784	DE573513	The "Credential History" button periodically disappears for various users.
33463017	DE570135	LDAP users are removed after LDAP errors during a refresh.
33477737	DE570601	PAM-CMN-0020 error when trying to view session logs.



Case Number	Internal Defect ID	Resolved Issue
33502602	DE573958	Receiving an Illegal Argument Exception error when accessing RDP to any Windows server.
33502648	DE574802	LDAP Device Group Refresh for one specific Group leads to a PAM-CMN-1172 error: "Your session has been terminated by a CA PAM administrator."
33520701	DE577434	SSH and RDP proxy Services are not getting started automatically when the Client Application path is set in Service.
33534837	DE578280	The RADIUS reauthentication prompt does not work in Threat Analytics for PAM 4.1.3.
33537429	DE580064	The Administrative Activities report immediately fails with an Error Code=803 and a NullPointerException.
33543414	DE579035	Assignable as "Yes" is incorrect for any unassignable User Groups, such as imported LDAP User Groups.
33550004	DE578917	The <b>Secrets &gt; Vaults</b> page is missing items.
33552223	DE579195	Daily process to purge binary logs older than 72 hours also purges all other binlogs, not just ones more than 72 hours old.
33552223	F133290	Add the ability to disallow group inherited permissions for users and API key.
33559656	DE582060	Unable to see the devices on an LDAP Device group.
33564431	DE581098	JAVA JDK interferes with PAM client 4.1.3.
33567728	DE581160	Some site VIPs stopped working after a 4.1.5 upgrade.
33568815	DE581696	Inconsistent Credential Source IDs in API Output
33572772	DE581659	Privileged accounts reports are not working post upgrade to 4.1.5.
33574824	DE581859	Customer is unable to copy a password to the clipboard in the PAM client.
33578770	DE582241	Cannot download and restore database backups on a MAC client.
33582217	DE582740	PAM nodes are unreachable but can still be pinged.
33578010	DE582477	SSO sessions are being reused by other users.

## Resolved Issues in 4.1.5

The following table lists the issues that are resolved in Release 4.1.5:

Case Number	Internal Defect ID	Resolved Issue
33406321	DE565052	Transparent login configuration is lost on a policy update.
33463974	DE568796	Hotfix 4.1.2.03 removes branding when applied to the system.
33514551	DE574727	UI not coming back from stopping the cluster
33506256	DE574061	Primary Appliance GUI stuck and not coming back after hot fix patch.
33492084	DE572188	RHEL9 with SecureCRT the related password is not transparently injected (that is user is being prompted to provide the Password)
33378964	DE564433	ILO Web portal failing to load tab.
33500828	DE575014	Login not happening and working automatically for TCP/UDP service.
33483399	DE571278	All staged patches purged on all nodes after applying one patch to secondary site nodes.
33437594	DE571188	Error 401 obtained in web browser after a logged in user properties are modified elsewhere

Case Number	Internal Defect ID	Resolved Issue
33453152	DE567972	User cannot login with some issued PIV cards. PKI authentication failed with the following error: Client chain certificate time-frame not valid
33448037	DE567134	Weaknesses detected during a PCI DSS scan for port 5249.
33461015	DE570295	Cannot Open Multiple SSH Sessions At Once
33478241	DE570563	If, when attempting to create a Target Account, the operation failed, the credential would be recorded in the metrics log for the failed creation. Only when the syslog was already configured (by selecting <b>Configuration, Logs, Syslog</b> ), the clear text password of the failed creation would be forwarded to syslog.
33462268	DE574330	PAM-CM-8014 error when modifying a secret.
33527388	DE576239	User Filter is not working as expected in Manage Vault.
33450215	DE567336	Error PAM-SEC-00017 appears when trying to save a secret.
33452974	DE568313	AD users temporarily deleted while patching the cluster.
33190981 / 33446426 / 3345742682 / 3345742682 / DE568592 / DE572351	DE5742682 / DE568592 / DE572351	Core dumps and restarts after inactivity when logging in through LDAP and RSA.
33282392	DE552803	User is unable to raise breakglass request from PAM Client.
33441179	DE566491	Long delays after upgrade to 4.1.2 for any activity involving listing of target accounts
33471375	DE569713	In 4.1.3, PVPs with Exclusive Checkout Cannot Be Updated Through the CLI
33398543	DE562340	Docker logging configuration update.
33453817	DE568384	PAM Manage Server Control error when creating a new policy. Specifically, any policy where you include an space before the CRLF will fail to be created.
33500417	DE573133	SAML IdP Metadata Refresher Cron job not running on PAM appliance.
33419367	DE566281	Accounts PDF Report incorrect.
33437557	DE566093	PIV CAC showing incorrect certificates.
33467542	DE569720	RDP Applet Exception when PAM Client on MacOS with Apple Chip: PAM Client on MacOS ARM64 Ventura cannot RDP to any Windows server.
33473462	DE570320	"Warning" dialogue but with no content in dashboard.
33447320	DE567462	Cannot delete any target server if any account with custom workflow is checked out
33395677	DE561984	Issue with accessing a specific Web Portal in PAM
33484068	DE571049	PAM-UI-2730 message syntax error.
33450855	DE569721	Maintenance Mode Turns on Automatically.
33498510	DE578207	Verification and target account password view are not showing on screen even though the user has CM privileges.
33492271	DE571948	An error on the access panel occurs when the "Set or Change local application" link in the secure tunnel popup is selected.
33434678	DE566435	Deleting CM objects such as target server from database is very slow.
33412582	DE572081	Poor A2A client performance.
33486218	DE572096	PAM GUI could not reboot appliance when applying a hotfix.
33495205	DE572409	PAM-CMN-5517 error appears when trying to modify a user.
33401357	DE562434	The UTA failover mechanism does not update the config map appropriately when switching the cluster primary sites. The multisite failover of UTA servers does not happen.



Case Number	Internal Defect ID	Resolved Issue
33393430 / 33138451	DE561989 / DE538741	Web Portal auto-logon stopped working.
33403046	DE562740	A2A 402 null errors are seen due to long processing time in PAM.
33412626 / 33141455	DE529787 / DE538447	A2A clients not notified on password updates in real time.
33519406	DE575780	Error Message not displaying while deleting Master Account.
33422520 / 33370144	DE564941 / DE559812	Long delays when joining a cluster or rebooting a node in the active cluster.
33535422	DE577282	After upgrade to 4.1.4 the SNMP v3 user get removed

## Resolved Issues in 4.1.4

The following table lists the issues that are resolved in Release 4.1.4:

Case Number	Internal Defect ID	Resolved Issue
33460514	DE568381	Dashboard does not load and reports the following error: "Unexpected token END OF FILE at position 0."
33424190, 33408206	DE564126, DE564764	UNIX target connector failures.

## Resolved Issues in 4.1.3

The following table lists the issues that are resolved in Release 4.1.3:

Case Number	Internal Defect ID	Resolved Issue
33380450	DE561227	Old cluster configuration found on removed node during cluster stop process, due to there being a risk of restarting the original database.
33291201 33316348	DE554423 DE554424	Increased CPU usage and performance issues occur after upgrading to PAM 4.1.1.
33401573	DE563081	The health page displays a node's status as OK, even while the node is still loading.
33409055	DE563208	Target Account selection broken for scp protocol option in DB backup scheduler.
33315067	DE556673	Selecting Credentials > Report > Activities to graph activities with thousands of events causes the system to hang.
33330092	DE557057	The PAM Agent port redirection is active even if Agent is stopped
33306178	DE552984	Session logs sent to the syslog are missing time zone information.
33308508	DE554754	A2A takes the interpreter name instead of the script name when running python2 or python3 scripts.
33320207	DE558502	Password rotation scheduled job for Nexus device fails while manual update is successful
33287995	DE551359	The LDAP refresh does not update all device groups, and is hung.
33385421	DE561225	User cannot download the ECDSA Private Key. Therefore, the User cannot download the key file to generate ECDSA certificates for their cluster.
33401157	DE562441	Approval workflow is not working across the cluster.
33408206 33424190	DE564126 DE564764	Failed to establish a communications channel to the remote host.
33398895	DE565158	Exclusive checkout not working with dual authorization.

Case Number	Internal Defect ID	Resolved Issue
33389593 33397005	DE561574 DE562066	The PAM client prompts to save the password for a target account when exiting a screen.
33404824	DE563495	Vaults are not decrypting Secrets
33391034	DE561500	Logstash container is not started when PAM is rebooted without shutting down Cluster.
33393424	DE561745	Deleting a PAM user leaves orphaned email recipients.
33393427	DE563496	Filtering devices by tags on Device > Manage Devices displays only the first page.
33296691	DE552544	LDAP refresh is not removing devices from LDAP groups that were deleted in Active Directory. The target device cannot be deleted when the custom connector has been deleted while there is an application with that application type in PAM.
33339379 33372710	DE556776 DE560320	User cannot use the internal RDP Applet to RDP to any servers
33357151	DE560991	Some devices export incorrect data flags for A2A devices.
33372255	DE559785	After upgrading to PAM 4.1.1, the Privileged Accounts report displays empty results.
33341409	DE556781	Users can access and browse Internet pages within the PAM Client, allowing users to by-pass their internet proxy.
33305029	DE553877	When a user inherits a CM group and is an approver for a PVP, modifying the user displays error PAM-CMN-0155.
33341109	DE557099	A PVP approver with roles and Credential Manager groups inherited through a user group can be removed from the user group without generating an error.
33093691 33319494 33134089 33106482	DE536414 DE554338 DE540076 DE535427	High CPU usage causing multiple problems, with session recording as the main suspect
33114722	DE538976	Cannot verify Azure accounts in PAM 4.0.1.
33362625	DE559581	Cluster node reboot makes the Management Console show an incorrect cluster status.
33366878 33393814	DE559518	Web Portal is not caching credentials across multiple tabs
33283665	DE551325	While the cluster service appears to be in sync, the primary node is inaccessible.
33242692	DE552779	A2A XML Credential Retrieval error: Cannot execute the cspmclient64.exe with the XML Option (-x) for any Unix Type Application Target Users.
33245266	DE548256	Erratic problems with ServiceNow integration related to multiple bc-fips JAR versions.
33325668	DE555952 DE555342	Password Authority error after switching user from Local CAC to LDAP Imported method
33407999	DE563310	Users listed as Dual Authorization users are not removed from the LDAP Group if they leave that LDAP group.

## Resolved Issues in 4.1.2

The following table lists the issues that are resolved in Release 4.1.2:

Case Number	Internal Defect ID	Resolved Issue
33082121	DE533603	PAM node becomes inaccessible due to thousands of stale xcd_spfd_wolfssl processes.
33124675	DE537765	PAM Agent authentication fails when the password includes a "&" character.

Case Number	Internal Defect ID	Resolved Issue
33140114	DE537866	Credential Manager reports do not honor time zone setting when using the "Today" option.
33155561	DE539518	Change of UPN does not get updated in cspm.user_filter_view table
33157811	DE539317	Auto-login to ACF2 MF with BlueZone client fails and exposes password.
33200818	DE546097	Rotating a password for an AD account with a forward slash (/) fails with a PAM-CM-0762 error
33204647	DE545447	PAM-CM-0964 error is seen when trying to add a generic secret to a vault.
33224536	DE547384	External API call GET /cspm/ext/rest/devices/{id}/policies returns an error after a target account is deleted.
33224672	DE545335	Potential vulnerability: HTTP Track/Trace method is enabled in PAM Windows Proxy.
33232801	DE546388	"Restore of local database content failed! Sleeping and retrying..." error on secondary nodes at cluster startup.
33238600	DE548615	A2A mapping navigation is not working properly.
33242683	DE547290	Inconsistent REST API responses related to internal groups for vaults are seen.
33248660	DE553291	Socket Filter Agent throws inappropriate "Access Denied" error messages when the user is only attempting to access an application on the local machine.
33248788	DE547840	Users remain as PVP approvers when user group is deleted.
33255102	DE548628	_JAVA_OPTIONS setting prevents PAM Client installer and executable from running.
33262155	DE549198 DE549545	SysInfo showing out of date information regarding cryptographic providers.
33264356	DE549181	JIT Access MS SQL returns an error from the Secondary site.
33277675	DE550450	API calls taking longer and causing high CPU utilization.
33292969	DE551840	TLS 1.2 Cipher selection only partially working.
33298241	DE552235	Cannot save session recording purge policy when a value is specified for the <b>Remove Restored Recordings Older than</b> option.
33300755	DE552518	PAM Windows Proxy server operations cause java.lang. NumberFormatException errors in PAM Tomcat log file.
33312158	DE553978	Sessions requiring Dual Authorization no longer work if the "Maximum Connection Idle Timeout (Minutes)" parameter is set to zero.
33254076 33257866	DE549357 DE548519	Web portal not working after upgrade.
33326765	DE555102	Search for request servers is failing with PAM-CMN-0039 error.
33307427	DE553100	External API call DELETE /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId} deletes incorrect target application.
33308720	DE553158	Vulnerability detected in A2A client version 4.12.3.
33319402	DE554250	Session recording service fails to start after reboot.
33247664	DE547612	(Alternate) Configuration utility not working.
33340925	DE556861	PAM will not save web portal service definitions with an exclamation mark ("!") – a valid special character – in the launch URL, displaying a "The url contains an invalid character" error.

## Resolved Vulnerabilities and Issues in 4.0.4

This content lists the vulnerabilities addressed and issues resolved in 4.0.4.

### Vulnerabilities Addressed

This section lists the vulnerabilities that were addressed in 4.0.4:

- CVE-2022-25625 - A malicious unauthorized PAM user can access the administration configuration data and change the values.
- Exploitable vulnerability: a scan revealed the HTTP Track/Trace method is being enabled for PAM Proxy. (Case Number: 33224672/Defect ID: DE545335)
- PAM Windows Proxy 4.0.3 vulnerability due to MS DLL - msvcr80.dll (CVE-2010-3190) (Case Number: 33191371/Defect ID: DE542546)

### Resolved Issues

The following table lists the issues that are resolved in Release 4.0.4:

Case Number	Defect ID	Description
33096730	DE535191	Sort order by host name does not work correctly.
33185343	DE542171	Authentication module for SCIM and other CSPM (Java) REST APIs does not take into account the authentication method API when examining the SAML scenario.
33087758	DE536543	PIV logins with PAM in FIPS mode do not work.
33202249	DE543170	API error on updating User Group from LDAP+RADIUS to LDAP+RSA.
33013715	DE527882	PAM AWS Session freezes when uploading to the s3 bucket.
33127557	DE536999	PAM-CM-1129 incorrectly states that password view request is autoconnect only.
33079322 33071256	DE532840 DE532337	Device creation via Rest API fails with internal server error 500/Using API to onboard devices can produce duplicate devices.
33108399	DE537405	Web portal cannot access without an update with learning mode.
33135166	DE537390	Rest API error creating policies with multiple RDP application services.
33108398	DE537756	"Credential Manager User Group" name changed to "ActiveMQ Group."
33140120	DE537883	Administrative Activities report has no recognizable order.
33160324	DE539318	AS400 connector uses non-SSL port 8476 with SSL/TLS enabled.
33157220	DE539133	Aliases not displaying when a user group is assigned to a credential group.
33134089	DE540076	Session disconnected due to a problem with session recording.
33197558	DE543412	Cannot delete new Credential Manager user groups (copies of predefined groups).
33196417	DE542762	SSH Certificate authentication fails when user has no defined email address.
33023767 33141455	DE529787 DE538447	A2A clients are not notified on password updates in real time.
33082121	DE533603	PAM node becomes inaccessible due to thousands of stale xcd_spfd_wolfssl processes.
33121139	DE536409	Cannot upload PAM upgrade patch to Management Console.
33155561	DE539518	UPN change causes user to lose custom views.
33141455 33204647	DE545447	PAM-CM-0964: Password policy not found when trying to create a secret.

Case Number	Defect ID	Description
33224536	DE547384	The REST API call GET /cspm/ext/rest/devices/{id}/policies returns an error after a target account is deleted.
33257866	DE548519	Web portal autologin is not working when there are multiple redirections before the login page.
33262155	DE549198 DE549545	The PAM UI and Sysinfo file incorrectly list "CA Technologies C-Security Kernel" as a cryptographic provider.

## Resolved Issues in 4.1.1

The following table lists the issues that are resolved in Release 4.1.1:

Internal Defect ID	Case Number	Resolved Issue
DE532440	32986225	Management Console cannot stage 4.0.x Upgrade Patches
DE528579	32987568	RADIUS login failure when using CHAP
DE529787	33023767	A2A clients are not notified on password updates in real time
DE530254	33042317	Account discovery error on HP-UX devices
DE532085	33064591	After updating the system certificate on a cluster node, the informational message that appears incorrectly states that you must <i>stop the cluster</i> and restart the appliance to make the certificate change take effect. You do not need to stop the cluster.
DE532844	33067185	Cannot discover accounts on machines that have had previous discoveries
DE532840	33079322	Device creation using External API fails with internal server error 500
DE536543	33087758	PIV logins with PAM in FIPS mode do not work.
DE535191	33096730	Sorting by Host Name not working in password approval list
DE534791	33103566	External API calls not working
DE527882	33013715	Uploading files to S3 on the AWS console freezes the session
DE537756	33108398	"Credential Manager User Group" name incorrectly changed to "ActiveMQ Group"
DE537405	33108399	Web portal autologin fails unless updated with learning mode
DE536792	33111464	List of target accounts incorrectly displayed for credential source when a user has Secrets Management roles
DE536409	33121139	Cannot upload PAM upgrade patch to Management Console
DE536418	33124294	External API not working
DE537351	33129022	Custom logo reverts to default setting after upgrade
DE537883	33140120	Administrative Activities report entries not properly ordered
DE537390	33135166	Rest API error creating policies with multiple RDP Application services
DE540076	33134089	Sessions disconnect due to a problem with session recording
DE539133	33157220	Aliases not displaying when user group is assigned to a credential group
DE539318	33160324	IBM i connector uses non-SSL port 8476 with SSL/TLS enabled
DE539974	3316195	Attempting to view A2A mapping fails with "PAM-CM-0039: Unable to perform operation. Please contact System Administrator" error
DE542171	33185343	SCIM-related API calls not working

Internal Defect ID	Case Number	Resolved Issue
DE543412	33197558	Cannot delete new Credential Manager user groups created by copying predefined groups
DE528965 DE532591	32955254 33073759	Node reboot negatively affects the cluster status in the Management Console
DE543170	33202249	API error on updating User Group from LDAP+RADIUS to LDAP+RSA

## Resolved Issues in 4.1

The following table lists the issues that are resolved in Release 4.1:

Internal Defect ID	Case Number	Resolved Issue
DE524280	32959034	PAM suddenly stops load-balancing incoming requests to a cluster member on the primary and secondary sites when the encrypted shared key on the cluster is not the same as the one on the VIP node.
DE526940	32967277	Archived audit logs are missing most accounting information.
DE526407	32987666	User accounts are getting disabled for no reason.
DE529787	33023767	Password changes are not being updated in a timely manner on A2A clients on which credential caching is enabled.
DE529663	33040420	Only one AWS Management Console session can be opened from the PAM Access page. Attempting to launch another session fails with a "You must first log out before logging into a different AWS account," even after closing the first session.
DE526914	32989235	Too many core dumps are getting stored on the PAM server (only the 20 latest should be preserved) because the rotation process cannot delete filenames that contain spaces or special characters.
DE525485	32940895	Autologin to web portal failing when using a target account configured with a password view policy with "Reason required for autoconnect" enabled.
DE529550	33030265	REST API calls to cluster interface GB8 fail.

## Resolved Issues in 4.0.3

The following table lists the issues that are resolved in Release 4.0.3:

Case Number	Defect ID	Resolved Issue
32820122	DE512341	Problem applying the upgrade package.
32940895	DE525485 DE525953	Web portal is not working with "Reason Required For Auto Connect" in PVP
32955254 33073759	DE528965 DE532591	Management Console not working.
32959034	DE524280	PAM suddenly stops load-balancing incoming requests to a cluster member on the primary and secondary sites when the encrypted shared key on the cluster is not the same as the one on the VIP node.
32967277	DE526940	Archived audit logs are missing most accounting information.
32987666	DE526407	User accounts are getting disabled for no reason.
32989235	DE526914	Too many core dumps are getting stored on the PAM server (only the 20 latest should be preserved) because the rotation process cannot delete filenames that contain spaces or special characters.

Case Number	Defect ID	Resolved Issue
33023767	DE529787	Password changes are not being updated in a timely manner on A2A clients on which credential caching is enabled.
33030265	DE529550 DE531588	Rest API calls to cluster interface GB8 fail after upgrade.
33040270	DE530736	PAM SAML SSO with JIT doesn't work on secondary PAM Appliance.
33040420	DE529663	Cannot open multiple AWS Management Console sessions after upgrade to 4.0.1.
33056234	DE531171 DE531376	Splunk syslog not showing session logs.
33064591	DE532085	Message that appears after changing a PAM server certificate incorrectly instructs you to stop the cluster before rebooting the server to apply the new certificate when you only need to reboot the server.
33067185	DE532844	After upgrade, PAM fails to discover new accounts on machines on which accounts had previously been discovered.
33078530	DE532968	The start and end dates returned by the "Data Range" value in report headers are incorrect (one year later than the actual dates).
33103566	DE534791	External API call "User" failing.

## Resolved Issues in 4.0.2

The following table lists the issues that are resolved in Release 4.0.2:

Case Number	Defect ID	Resolved Issue
32233314 / 32383169	DE482249	Proxy performance improvements.
32785147	DE510015	Passwords in PAM cannot be viewed or used for auto-connect.
32490309	DE493997	Windows Proxy from a different domain incorrectly used, resulting in the failure of password verification or update attempts.
32563475	DE503744	Auto-login to a ZOS Mainframe not working when using a model 5 terminal type.
32610867	DE498310	SSH Keys are rotating but not saving to the database.
32638752	DE502730	Unable to execute SSH commands if another SSH is already executing commands.
32671486	DE505743	Added A2A Scripts disappears from the list of scripts available. It is not located in any mapping and it is not searchable. Subsequently unable to remove A2A request device in GUI as well.
32714267	DE508360	Credential Manager reports display incorrect or future dates for columns. such as Password Created.
32747867	DE509503	PAM client is not getting launched using explicit proxy setting
32752042 / 32763845	DE507465 / DE508590	PAM Client prevents further SSH applet connections after an applet tries to connect to unreachable target device
32776382	DE509870	Users cannot login to the PAM client on macOS due to loopback address errors.
32779575	DE510873	Incorrect information in View Password Requests report
32789121	DE510233	LDAP user group refresh problem where users get deleted.
32802876	DE512520	A premature cluster start after an accidental stop causes a full outage for all nodes in the cluster.
32809511	DE518338	Delegated admin has problems adding users to groups.



Case Number	Defect ID	Resolved Issue
32809895	DE511409	SAML authentication problems due to missing TAP Administrators user group
32811228	DE511974	DoD Strong Password bug in PAM4.0
32814484	DE512177	Tomcat session recording catalina.out file size becomes too large when setting the Applet Log Level to Debug.
32827869	DE512910	Access side syslog message truncated to 1024 characters
32789634	DE510261	Cluster master is inaccessible after a brief replication problem.
32828253	DE513634	Problem loading session recording viewing screen.
32831195	DE513252	Session recordings stuck in Encoding In-Progress state
32848774 / 32852643	DE514993 / DE515243	PAM is not updating group membership of the user based on the IDP response
32854120	DE516709	Policy Manage GUI while Adding/Updating policy creates unexpected results.
32854290	DE515213	Getting blank results when running a Bulk Network Scan.
32855889	DE516045	Custom Connector Target Manager only sends one master account to the custom connector.
32858788 / 32884203	DE517067 / DE517915	The following command generate a Request error: listPasswordViewRequestByRequestorSummary
32864079	DE515971	Login Integration does not work when an LDAP user's OU contains an ampersand (&) in the string.
32937420	DE522439	Web Portal with long service name fails if Route Through PAM is checked
32865962	DE517268	After upgrading to PAM 4.0 or 4.0.1, SCIM related API calls no longer work. The following error message appears: "PAM-CM-4075: Error processing request. Please contact Administrator."
32878934	DE518613	Ability to list Policy deployed and Assigned is not working when attempting using the RestAPI.
32880524	DE521176	Alias listing is unavailable in global administrator role.
32881227	DE518202	Sorting by columns is incorrect.
32886091	DE518049	Users unable to login with "CA PAM is starting up" error.
32894799	DE519841	Unable to access web portal from PAM appliances when using IE
32906058	DE520239	Cluster node stuck in a quorum loss mode due to stale marker files.
32900507	DE520217	Cluster Logs not viewable
32908070	DE520357 / DE526157	Rotating passwords with the Use elevated privileges with authentication enabled produces a "PAM-CM-1349" error.
32910260	DE520553	Vulnerability exposed via PAM online help in PAM UI
32914638	DE521200	VNC applet does not work with VNC authentication.
32914749	DE520579	A2A installer on Windows creates a bad Perl library CSPM_CLIENT_WIN.pm
32914976	DE521328	Windows Proxy Connection Status not reflecting lastupdate and date attributes.
32918907	DE520812	Cannot apply hotfix after uploading to PAM.
32925384	DE521365	Uninformative PAM-UI-2401 error logged when user deletion fails
32927723	DE521644	AIDE report received from PAM appliance, warning about a change in the /var/www/htdocs/uag/gatekeeper.ini file.
32937499	DE522434	Improper Policy Export Formatting causes a PAM-CMN-0668 error when importing the CSV
32937506	DE522436	LDAP User Groups are not Exported to a CSV file.



Case Number	Defect ID	Resolved Issue
32941242	DE526696	A utility group cannot be deleted if a PAM appliance is from an upgrade, resulting in a Utility Group Delete Error.
32950088	DE523607	Fix for log4j vulnerability (EventForwarder).
32964959 / 32967539	DE524228 / DE524391	Credential Manager Reports show incorrect year.
32968279	DE524434	300+ Active users were incorrectly flagged and disabled due to inactivity.
32974762	DE525066	New AWS Access key displays only the key ID to users instead of the friendly name.
32978211	DE526604 / DE525318	Log4J jar update required for the PAM client.
32978647	DE528037	Trying to upload IDP metadata file into PAM displays error.
32980978	DE526583	TCF with a uiDefinition using a TARGET Account cannot remove an assigned account in PAM 4.0.
32982908	DE525925	Only some target accounts appear in a list associated with a server host name.
32986498	DE525791	Need log4j patch with the latest log4j2 version 2.17.1.
32860526 / 32889747	DE516465 / DE518511	PAM-CMN-0155 error appears when removing CM Group from user due to PVP, despite user belonging to the user group with same CM group. Cannot update (unlock) user with inherited approver role.
33010780	DE527886	Fixed Access Page Filter Columns availability.
33019179	DE528189	Problems with Radius passcode prompt after upgrading from 3.4.2 to 4.0.1.
32820122	DE512341	Problem applying the upgrade package.
33060174	DE531472	HDD 99%; GUI not accessible after upgrade to 4.0.2

## Resolved Issues in 4.0.1

The following table lists the issues that are resolved in Release 4.0.1:

Case Number	Defect ID	Resolved Issue
20055428	DE448496	Discover Services that Use AD Accounts.
20305839 01258661 31800936	DE451560, DE409443, DE451579	Idle Sessions are not being terminated.
32095417	DE471602	Auto-login not working consistently with TN3270
32105667	DE470660	PAM UI reporting a "communication failure" error when password update takes more than 2 minutes.
32192407	DE485417	PAM Agent Login Problem
32193181	DE485677	Windows Proxy fails to update the scheduled task credentials for AD accounts.
32236359	DE484446	Every LDAP login to Secondary Node leads to two internal SYSTEM-related error messages.
32317657	DE482868	Attempt to delete a user who defined a custom session log report leaves a corrupt user behind
32328545	DE485272	When customizing a session log report, the XSSO and SSO transaction types are missing from the <b>Available Transactions</b> list on the <b>Transactions</b> tab of the <b>Create Report</b> dialog.
32375184	DE489607	Device Import/Export Failure
32446011	DE488413	Moving a target account configured for view in a policy to a different target app corrupts the policy.

Case Number	Defect ID	Resolved Issue
32448660	DE488977	PAM client pops up a "Login failed" message and closes the web portal on acknowledgment even though login was successful.
32451951	DE489945	The comments that are entered for Retrospective Approval are missing on the approval pop-up.
32489126	DE496979	Customizing the email body of password view policy causes duplicates emails.
32514173	DE492397	Problems with default AWS Management Console SSO service access list in PAM
32514991	DE492544	Documented filter not working for CLI command listTargetAccounts.
32519909	DE503233	PAM-CMN-0020/PAM-CMN-2293 errors occur and the user cannot log in to the target if "<" or ">" is included in the Password view reason.
32521806	DE493750	Query filters not working after customizing the status mapping in NIM for ServiceNow.
32534674	DE499203	Branch user unable to log in after removed from a different domain group in a Microsoft Active Directory with multiple Domains
32539544	DE495646	PAM Agent loading slowly
32570723	DE496953	Syslog Forwarder Message Format broken
32570756	DE494895	PAM allows deletion of device with target accounts that manage other accounts, leaving broken accounts behind.
32579168	DE495931	Unauthorized Access to Service Controller messages when access session terminations should be logged.
32608331	DE500455	RDP application keeps showing the previous RDP application session.
32615613	DE499657	SecureCRT prompts for password instead of passcode.
32624867	DE498458	User import fails when their first name exceeds 30 characters.
32629271	DE501994	Cannot log in with PAM Agent when "User Must Accept License" is checked.
32632737	DE499783	Management Console not staging tasks
32633111	DE499165	Old DB backup used for cluster resync.
32653380	DE500287	Cluster restore to DB failures are not caught.
32676592	DE501702	CSPM running out of memory
32687188	DE502550	Accounts CSV report still contains many entries spanning two lines in 3.4.3.
32705829	DE504075	PAM cannot manage MSSQL accounts with a dash in the name.
32705872	DE503759	When a Java app runs a remote CLI command against PAM on a secondary site node, that node becomes unavailable.
32707139	DE503715	Files with Special Characters being created
32707978	DE503873	Over time, attempts to update and verify target accounts stop working and the PAM administrator receives a "communication failure" error. Also, accessing session recordings causes excessively high memory usage.
32708252	DE503776	PAM Console fails to start.
32709768	DE504247	AD account update breaks services and tasks when Proxy is unavailable.
32735389	DE506904	Leaving and rejoining a cluster corrupts the PAM instance and prevents the UI from starting.
32741194	DE506662	Compacting the database using an outdated method from an older version of MySQL that did not officially support any native means to compact the database.
32743243	DE506255	Improper access for users with multiple Credential Manager roles

Case Number	Defect ID	Resolved Issue
32751528	DE507244	Scheduled Jobs not running at the correct time.
32753632	DE507293	Functionally unnecessary IPv6 TCP ports 9092 and 9093 are open and listening in PAM 4.0 and should be closed.
32769335	DE509522	DEV appliance went down when its custom connector became unavailable.
32777404	DE509262	Scheduled job not honoring "Use Same Password" flag if the first account update fails.
32778828	DE509721	Radius MFA authentication fails when the password length exceeds 48 characters.
32783777	DE509421	Cannot view passwords after (cluster) restart.
32823462	DE513563	Unable to connect to an Oracle DB using TLS 1.2.
32828088	DE513689	Upgrade fails over existing device entries with a uag.host.os value that does not match any OS type in uag.os.
32837549	DE514899	Setting the <b>Disable Inactive after (Days)</b> option to zero ("0") on the <b>Global Settings</b> panel <b>Accounts</b> tab is intended to <i>prevent</i> users from ever being disabled due to inactivity. However, it is actually causing all users (except the "super" admin) to be disabled after zero days of inactivity.
32838772	DE515155	Not able to change the default password for the config user.
32255005, 32428015	DE481379, DE498725	Unable to synchronize AWS Key Pair accounts
32387108, 32689321	DE490271, DE503075	Verify using account not working when used a custom Unix prompt for the other account
32400096, 32437216	DE487536, DE488190	Session hangs after Transparent Login from Default SSH App.
32511527, 32567759	DE493913, DE500445	Command-Line Filter Violations and Session Log Updates not happening.
32528090, 32511285	DE493419, DE493987	SSH access using PAM applet got disconnected randomly.
32615976, 32633152	DE498218, DE499400, DE500342	Automatic login using the SSH Tunnel service fails after upgrade.
32656828, 32541064	DE501493, DE500778	Thousands of "session_recording" messages are recorded in the transaction logs when users access any of the defined Web Portals.
32695378, 32740566	DE503026	UI runs slowly after an LDAP device refresh runs.
32780662, 32840634	DE512345, DE514051	Authentication issue on account (PAM)
32922527	DE514260, DE521083	Disabled DSApiUser/MCApiUser user accounts prevent Utility Servers from starting.
N/A	DE497234	Database backup for quorum loss mode fails.

## Resolved Issues in 4.0

The following table lists the issues that were resolved in Release 4.0:

Case Number	Defect ID	Resolved Issue
31819149	DE456073	Incorrect auto archive warning messages appear in the PAM Client dashboard even after a successful auto archive: PAM-CMN-3136: Metrics auto archive failed. Please check Settings, Credential Manager Settings, Auto-Archive. PAM-CMN-3137: Audit Log auto archive failed. Please check Settings, Credential Manager Settings, Auto-Archive.
32170627	DE475046	Session recording not working on one of three primary site nodes

Case Number	Defect ID	Resolved Issue
32509351	DE492450	XSIE Extracts do not export Target Accounts
32549376	DE495930	After upgrading to 3.4.2 the session log export to an external database may have duplicate entries

## New and Revised External API Calls in 4.x and 4.x.x Releases

This content lists the new and revised External API calls in PAM 4.0 and later 4.x and 4.x.x releases. For detailed information about any of these calls, refer to the [API Explorer](#) in the product UI.

### New Calls in 4.1.7

The following calls were added in 4.1.7 and are applicable in all later (by date) 4.1.x and 4.x releases:

Method	Function
POST /cspm/ext/rest/credentialUserGroups	Provide support for managing Credential Manager credential groups using the External API.
PUT /cspm/ext/rest/credentialUserGroups/{id}/users	
PUT /cspm/ext/rest/credentialUserGroups/name/{name}/users	
PUT /cspm/ext/rest/credentialUserGroups/{id}/userGroups	
PUT /cspm/ext/rest/credentialUserGroups/name/{name}/userGroups	
PUT /cspm/ext/rest/credentialUserGroups/name/{name}	
PUT /cspm/ext/rest/credentialUserGroups/name/{name}	
GET /cspm/ext/rest/credentialUserGroups/userName	
GET /cspm/ext/rest/credentialUserGroups/{id}/eligibleUsers	
GET /cspm/ext/rest/credentialUserGroups/userName/{name}/eligibleUsers	
GET /cspm/ext/rest/credentialUserGroups/{id}	
GET /cspm/ext/rest/credentialUserGroups/{id}/protectedUserGroups	
GET /cspm/ext/rest/credentialUserGroups/name{name}/protectedUserGroups	
GET /cspm/ext/rest/credentialUserGroups/{id}/protectedUsers	
GET /cspm/ext/rest/credentialUserGroups/name{name}/protectedUsers	
GET /cspm/ext/rest/credentialUserGroups/name/{name}/eligibleUserGroups	

Method	Function
GET /cspm/ext/rest/credentialUserGroups/{id}/eligibleUserGroups	
GET /cspm/ext/rest/credentialUserGroups	
GET /cspm/ext/rest/credentialUserGroups/name/{name}	
DELETE /cspm/ext/rest/credentialUserGroups/{id}	
DELETE /cspm/ext/rest/credentialUserGroups/name/{name}	
GET /cspm/ext/rest/credentialRoles	<a href="#">Get Credential Manager Roles Using the External API.</a>

### Revised Calls in 4.1.7

The following calls External API methods were revised in 4.1.7 and the revisions are applicable in all later (by date) 4.x and 4.x.x releases

Call	Revision
POST /api.php/v1/devices.json/{id}/targetApplications PUT /api.php/v1/devices.json/{id}/targetApplications	Added support for the following target applications: <ul style="list-style-type: none"> <li><a href="#">Windows SSH Key</a></li> <li><a href="#">Windows SSH Password</a></li> </ul> (Select the corresponding entry for details of the new configuration field attributes introduced by each application type.)

### Revised Calls in 4.1.6

The following calls were revised in 4.1.6 and the revisions are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Revision
POST /api.php/v1/users.json	Now allows you to <a href="#">specify the Access Manager user groups from which an API Key inherits roles</a> by adding or removing their IDs from the <code>groupIds</code> array that has been added to the <code>apiKeys</code> array.
PUT /api.php/v1/users.json	Now allows you to <a href="#">specify the Access Manager user groups from which an API Key inherits roles</a> by adding or removing their IDs from the <code>groupIds</code> array that has been added to the <code>apiKeys</code> array.
GET /api.php/v1/users.json	Now returns the <a href="#">IDs of Access Manager user groups from which an API key inherits roles</a> in the <code>groupIds</code> array that has been added to the <code>apiKeys</code> array.
GET /api.php/v1/users.json{id}	Now returns the <a href="#">IDs of Access Manager user groups from which an API key inherits roles</a> in the <code>groupIds</code> array that has been added to the <code>apiKeys</code> array.

## Revised Calls in 4.1.5

The following calls were revised in 4.1.5 and the revisions are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Revision
GET /cspm/ext/rest/config/splunk/splunksettings	"JSON" is now a supported value for the field <code>splunkMessageFormat</code> .
PUT /cspm/ext/rest/config/splunk/splunksettings	
GET /cspm/ext/rest/config/logs/syslog	"JSON" is now a supported value for the field <code>syslogMessageFormat</code> .
PUT /cspm/ext/rest/config/logs/syslog	
GET /api.php/v1/devices.json/{id}/targetApplications	Now returns <code>enableKerberos</code> in the response body of target applications of type <a href="#">Active Directory</a> or <a href="#">Windows Remote</a> .
GET /api.php/v1/devices.json/{id}/targetApplications/{applicationId}	
POST /api.php/v1/devices.json/{id}/targetApplications	Now allows you to enable Kerberos authentication when creating an <a href="#">Active Directory</a> or <a href="#">Windows Remote</a> target application. To do so, add <code>"enableKerberos": "t"</code> to the request body. When creating a Kerberos-enabled <a href="#">Windows Remote</a> target application, you can enable it to support a different domain controller lookup type than an existing Kerberos-enabled Windows Remote target application in the same domain. To do so, add <code>"overrideDnsType": "t"</code> to the request body.
PUT /api.php/v1/devices.json/{id}/targetApplications	Now allows you to enable or disable Kerberos authentication when updating an <a href="#">Active Directory</a> or <a href="#">Windows Remote</a> target application. To do so, add <code>"enableKerberos": "t"</code> to the request body. When updating a Kerberos-enabled <a href="#">Windows Remote</a> target application, you can now modify the value of an existing <code>overrideDnsType</code> ("t" or "f") entry in the request body to change whether it supports a different domain controller lookup type than an existing Kerberos-enabled Windows Remote target application in the same domain.
GET /api.php/v1/users.json	Now returns an <code>extendedIdentities</code> parameter, which lists alternate accounts that are configured to access RDP applets, Mainframe applets, and Azure SQL Managed Instances. Possible list entries are RDP User Name, Mainframe Display Name, and Azure User Name.
GET /api.php/v1/users.json{id}	Now returns an <code>extendedIdentities</code> parameter, which lists alternate accounts that are configured to access RDP applets, Mainframe applets, and Azure SQL Managed Instances. Possible list entries are RDP User Name, Mainframe Display Name, and Azure User Name.

Call	Revision
POST /api.php/v1/users.json	Now allows you to optionally specify an <code>extendedIdentities</code> parameter that specifies an alternate account to use to access RDP applets, Mainframe applets, or Azure SQL Managed Instances. Possible list entries are RDP User Name , Mainframe Display Name , and Azure User Name .
PUT /api.php/v1/users.json	Now allows you to modify an <code>extendedIdentities</code> parameter, specifying an alternate account to use to access RDP applets, Mainframe applets, or Azure SQL Managed Instances. Possible list entries are RDP User Name , Mainframe Display Name , and Azure User Name .

### New Calls in 4.1.4

The following calls were added in 4.1.4 and are applicable in all later (by date) 4.1.x and 4.x releases:

Call	Function
GET /cspm/ext/rest/config/network/container/local/ipv6	Get the <a href="#">Local PAM Container IPv6 Subnet CIDR</a> .
PUT /cspm/ext/rest/config/network/container/local/ipv6	Set the <a href="#">Local PAM Container IPv6 Subnet CIDR</a> .

### Replaced Calls in 4.1.4

The following calls were replaced in 4.1.4. The revisions are applicable in all later 4.1.x and 4.x releases:

Call	Revision
<ul style="list-style-type: none"> <li><b>Old:</b> GET /cspm/ext/rest/config/network/docker/local/status</li> <li><b>New:</b> GET /cspm/ext/rest/config/network/container/local/status</li> </ul>	<ul style="list-style-type: none"> <li><b>Old:</b> Returned the status of the local PAM Docker daemon.</li> <li><b>New:</b> Returns the status of the <a href="#">Local PAM Container daemon</a>.</li> </ul>
<ul style="list-style-type: none"> <li><b>Old:</b> GET /cspm/ext/rest/config/network/docker/local</li> <li><b>New:</b> GET /cspm/ext/rest/config/network/container/local/ipv4</li> </ul>	<ul style="list-style-type: none"> <li><b>Old:</b> Returned the local PAM Docker CIDR.</li> <li><b>New:</b> Returns the <a href="#">Local PAM Container IPv4 network bridge address</a>.</li> </ul>
<ul style="list-style-type: none"> <li><b>Old:</b> GET /cspm/ext/rest/config/network/docker/utilityAppliances</li> <li><b>New:</b> GET /cspm/ext/rest/config/network/container/utilityAppliances</li> </ul>	<ul style="list-style-type: none"> <li><b>Old:</b> Returned the Utility Appliances Docker CIDR.</li> <li><b>New:</b> Returns the <a href="#">Utility Appliance Container IPv4 network bridge address</a>.</li> </ul>
<ul style="list-style-type: none"> <li><b>Old:</b> PUT /cspm/ext/rest/config/network/docker/local</li> <li><b>New:</b> PUT /cspm/ext/rest/config/network/container/local/ipv4</li> </ul>	<ul style="list-style-type: none"> <li><b>Old:</b> Set the local PAM Docker CIDR.</li> <li><b>New:</b> Sets the <a href="#">Local PAM Container IPv4 network bridge address</a>.</li> </ul>

Call	Revision
<ul style="list-style-type: none"> <li><b>Old:</b> PUT /cspm/ext/rest/config/network/docker/utilityAppliances</li> <li><b>New:</b> PUT /cspm/ext/rest/config/network/container/utilityAppliances</li> </ul>	<ul style="list-style-type: none"> <li><b>Old:</b> Set the Utility Appliance Docker CIDR.</li> <li><b>New:</b> Sets the <a href="#">Utility Appliance Container IPv4 network bridge address</a>.</li> </ul>

### New Calls in 4.1.3

The following calls were added in 4.1.3 and are applicable in all later (by date) 4.1.x and 4.x releases:

Call	Function
GET /cspm/ext/rest/system/userLoginMessage/{id}	Get the configured <a href="#">login message</a> with the specified <i>id</i> .
GET /cspm/ext/rest/system/userLoginMessage	Get a list of <a href="#">login messages</a> . This list has either zero or one message.
PUT /cspm/ext/rest/system/userLoginMessage/{id}	Set or update the <a href="#">login message</a> with the specified <i>id</i> .
POST /system/unhideUserLoginMessageForAllUsers	Unhide a <a href="#">login message</a> configured for all users.
POST /cspm/ext/rest/user/hideUserLoginMessage	Hide the <a href="#">login message</a> for the user who is associated with the API key that is used for authentication.
POST /cspm/ext/rest/user/unhideUserLoginMessage	Unhide the <a href="#">login message</a> for the user who is associated with the API key that is used for authentication.

### Revised Calls in 4.1.3

The following calls were revised in 4.1.3 and the revisions are applicable in all later 4.1.x and 4.x releases:

Call	Revision
GET /api.php/v1/services.json/{id} GET /api.php/v1/services/tcpudp.json	All GET methods now accept the <code>hideCredentialLink</code> field in <code>fields</code> input parameters, and returns the <code>hideCredentialLink</code> value for service objects.
GET /cspm/ext/rest/configProperties	Now returns details of a configured <a href="#">login message</a> : "name" : "userLoginMessage"
POST /api.php/v1/services/tcpudp.json PUT /api.php/v1/services/tcpudp.json	Both support the new optional parameter <code>hideCredentialLink</code> . If <code>View Credential</code> is disallowed when establishing a service, specify <code>t</code> to prevent a <code>View Credential</code> link from appearing on the Access page. The default is <code>f</code> , to allow a <code>View Credential</code> link. This parameter only applies to TCP/UDP Services with the <code>Application Protocol Disabled</code> .



## New Calls in 4.1.2

The following calls were added in 4.1.2 and are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Function
GET /cspm/ext/rest/proxies/web	Get all web proxies. Originally implemented in 4.0.4.
GET /cspm/ext/rest/proxies/web/{id}	Retrieve the web proxy with the specified id. Originally implemented in 4.0.4.
POST /cspm/ext/rest/proxies/web	Create a web proxy. Originally implemented in 4.0.4.
PUT /cspm/ext/rest/proxies/web/{id}	Update a web proxy. Originally implemented in 4.0.4.
DELETE /cspm/ext/rest/proxies/web/{id}	Delete the specified web proxy. Originally implemented in 4.0.4.

## Revised Calls in 4.1.2

The following calls were revised in 4.1.2 and the revisions are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Revision
GET /api.php/v1/devices.json/{id}/targetApplication	<p>Previously, you required the <b>Read Devices</b> Access Control privilege (and appropriate Credential Manager privileges) to use these calls to target applications or target accounts for a device. This was inconsistent with the PAM UI, on which you did <i>not</i> require the Read Devices privilege to create, update, or target applications or accounts. These calls are now compatible with the UI – the Read Devices privilege is no longer required to perform these operations using the external REST API.</p> <p>The <b>Read Devices</b> privilege is still required to obtain the Device ID, which is required for all target application and target account calls.</p>
GET /api.php/v1/devices.json/{id}/targetApplications/{applicationId}	
GET /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts	
GET /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts/{accountId}	
POST /api.php/v1/devices.json/{id}/targetApplications	
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts	
PUT /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts	
PUT /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts	
DELETE /api.php/v1/devices.json/{id}/targetApplications	
/api.php/v1/devices.json/{id}/targetApplications	
GET /api.php/v1/services.json	Now optionally includes webProxyID and webProxyName . Originally implemented in 4.0.4.

Call	Revision
GET /api.php/v1/services.json/{id}	Now optionally includes webProxyID and webProxyName . Originally implemented in 4.0.4.
POST /api.php/v1/services/tcpudp.json	The POST body can now optionally include webProxyID or webProxyName , or both. Originally implemented in 4.0.4.
PUT /api.php/v1/services/tcpudp.json	The PUT body can now optionally include webProxyID or webProxyName , or both. Originally implemented in 4.0.4.

### New Calls in 4.1.1

The following calls were added in 4.1.1 and are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Revision
GET /cspm/ext/rest/config/crypto/tlsciphers{version}	Get TLS cipher suites that are currently enabled and disabled.
PUT /cspm/ext/rest/config/crypto/tlsciphers{version}	Enable or disable TLS cipher suites.
POST /api.php/v1/system/processes/sessionRecordingPurging.json	Launches the session recording purge process for the session recording mount attached to the current instance of PAM.
POST /api.php/v1/system/processes/sessionRecordingReconciliation.json	Launches all types of session reconciliation purge (mostRecent, recoverPAM, allOthers) for the session recording mount attached to the current instance of PAM.
PUT /cspm/ext/rest/config/logs/sessionRecordingPurge	Update session recording purge settings.

### Revised Calls in 4.1.1

The following calls were revised in 4.1.1 and the revisions are applicable in all later (by date) 4.x and 4.x.x releases:

Call	Revision
GET /api.php/v1/passwords/viewRequests.json	Added new connectionTimeout filter. If specified in the request, any timeout greater or equal to the specified value is returned. In any case, the connection timeout is now returned for all relevant password view requests.
GET /api.php/v1/policies.json/	Now returns hasExtendedTimeout indicating whether policies have the <b>Extended Timeout</b> option set with a value of <i>t</i> (for true) or <i>f</i> (for false).
GET /api.php/v1/policies.json/{id}	Now returns hasExtendedTimeout indicating whether the specified policy has the <b>Extended Timeout</b> option set with a value of <i>t</i> (for true) or <i>f</i> (for false).
GET /api.php/v1/policies.json/{userOrGroupId}/{deviceOrGroupId}	Now returns hasExtendedTimeout indicating whether the specified policy has the <b>Extended Timeout</b> option set with a value of <i>t</i> (for true) or <i>f</i> (for false).
POST /api.php/v1/policies.json/{userOrGroupId}/{deviceOrGroupId}	Added support for configuring extended timeout functionality by specifying a value of <i>t</i> (for true) or <i>f</i> (for false) in the hasExtendedTimeout parameter.

Call	Revision
GET /api.php/v1/services/tcpudp.json POST /api.php/v1/services/tcpudp.json PUT /api.php/v1/services/tcpudp.json	Added support for keepaliveInterval, SCP, SFTP, and publicKeyAuthentication for the SSH Application protocol type.
DELETE /api.php/v1/passwords/checkedIn.json/{accountId}	New error messages if the account does not have checkin enabled or have exclusive checkout enabled.

### New Calls in 4.0

The following calls were added in release 4.0 and are available in all later (by date) 4.x and 4.x.x releases:

Call	Description
GET /api.php/v1/deviceGroups.json/{id}/utilityGroup	For the Utility GroupD specified by {id}, returns information on the internal state of the individual Utility Appliances that make up the utility group.
GET /api.php/v1/devices.json/{id}/unabConfig PUT /api.php/v1/devices.json/{id}/unabConfig	Get or update the UNAB config tokens for the device that is specified by {id}.
GET /api.php/v1/deviceGroups.json/{id}/unabConfig PUT /api.php/v1/deviceGroups.json/{id}/unabConfig	Get or update the UNAB config tokens for the device group that is specified by {id}.
GET /cspm/ext/rest/sc/policies/audit	Get the Server Control Policy Deployment Audit Log.
GET /cspm/ext/rest/sc/policies/{policyId}/version/current	Get the current Server Control Policy Script version by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/versions	Get Server Control Policy Script versions by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/version/{versionId}	Get a specific Server Control Policy Script version by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/assignment	Get assigned devices and device group to a policy by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/assignment/devices	Get assigned devices to a Server Control Policy by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/upgradable/devices	Get a list of devices that can be upgraded to the latest version of Server Control Policy by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}	Get a specific Server Control Policy by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/downgradable/devices	Get a list of devices that can be downgraded to the specified policy version by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/assignment/deviceGroups	Get assigned device groups to a Server Control Policy by Policy id.
GET /cspm/ext/rest/sc/policies/{policyId}/upgradable/deviceGroups	Get a list of device groups that can be upgraded by Policy id.
GET /cspm/ext/rest/sc/policies	Get Server Control Policies
POST /cspm/ext/rest/sc/policies	Create a Server Control Policy and initial Script version.
POST /cspm/ext/rest/sc/policies/{policyId}/version	Create a Server Control Policy Script version.

Call	Description
PUT /cspm/ext/rest/sc/policies/{policyId}/assignment	Assign devices and device groups to the latest finalized Server Control Policy Script version.
PUT /cspm/ext/rest/sc/policies/{policyId}	Update a Server Control Policy description.
PUT /cspm/ext/rest/sc/policies/{policyId}/assignment/upgrade	Upgrade devices to the latest finalized Server Control Policy Script version.
PUT /cspm/ext/rest/sc/policies/{policyId}/assignment/downgrade	Downgrade devices to the specified Server Control Policy Script version
PUT /cspm/ext/rest/sc/policies/{policyId}/version	Update a Server Control Policy Script version.
DELETE /cspm/ext/rest/sc/policies/{policyId}/assignment	Unassign devices and device groups from a Server Control Policy.
DELETE /cspm/ext/rest/sc/policies/{policyId}	Delete a specific Server Control Policy by id.
GET /cspm/ext/rest/sc/unab/policies/audit	Get the UNAB Policy Deployment Audit Log.
GET /cspm/ext/rest/sc/unab/policies/{policyId}	Get a specific UNAB Policy by Policy id.
GET /cspm/ext/rest/sc/unab/policies	Get UNAB Policies.
POST /cspm/ext/rest/sc/unab/policies	Create a UNAB Policy.
PUT /cspm/ext/rest/sc/unab/policies/{policyId}	Update the associated users and user groups of a UNAB Policy.
DELETE /cspm/ext/rest/sc/unab/policies/{policyId}	Delete a specific UNAB Policy by id.

### Revised Calls in 4.0

The following calls were revised in 4.0 and the revisions are applicable in all later 4.x releases:

Call	Revision
GET /api.php/v1/deviceGroups.json/ PUT /api.php/v1/deviceGroups.json/	Added new provision type "Utility Group" to represent PAM SC Utility Groups.
POST /api.php/v1/devices.json/{id}/targetApplications PUT /api.php/v1/devices.json/{id}/targetApplications	Added support for three new values in the applicationType field: <ul style="list-style-type: none"> <li><a href="#">windows (Windows Proxy)</a></li> <li><a href="#">windowsRemoteAgent (Windows Remote)</a></li> <li><a href="#">windowsDomainService (Active Directory)</a></li> </ul> (Select the corresponding entry for details of the new configuration field attributes introduced by each application type.)
GET /api.php/v1/services/tcpudp.json POST /api.php/v1/services/tcpudp.json PUT /api.php/v1/services/tcpudp.json	Added support for keepaliveInterval, SCP, SFTP, and publicKeyAuthentication for the SSH Application protocol type.
DELETE /api.php/v1/passwords/checkedIn.json/{accountId}	New error messages if account does not have checkin enabled or have exclusive checkout enabled. Function

## Revised Credential Manager CLI Commands in 4.x Releases

### Revised Call in 4.1.7

The following call was revised in 4.1.7 and this revision is applicable in all later 4.x releases:

Command	Revision
<code>addTargetApplication</code>	<p>Added support for the following target applications:</p> <ul style="list-style-type: none"> <li><a href="#">Windows SSH Key</a></li> <li><a href="#">Windows SSH Password</a></li> </ul> <p>(Select the corresponding entry for details of the new configuration field attributes introduced by each application type.)</p>

### Revised Calls in 4.1.5

The following calls were revised in 4.1.5 and these revisions are applicable in all later 4.x releases:

Command	Revision
<code>addTargetApplication</code>	<p>When adding an Active Directory or Windows Remote target application, you can use the optional <code>Attribute.enableKerberos</code> parameter to enable or disable Kerberos authentication.</p> <p>When adding a Windows Remote target application with Kerberos enabled, you can also use the optional <code>Attribute.overrideDnsType</code> parameter to specify whether to allow a different DNS lookup type for this target application than for others in the same domain.</p> <p>For more information, see <a href="#">Active Directory Target CLI Configuration</a> and <a href="#">Windows Remote Target Connector CLI Configuration</a>.</p> <p>When adding an MSSQL Azure Managed Instance target application, you must use the following parameters with the specified values:</p> <ul style="list-style-type: none"> <li><code>TargetApplication.type : mssqlAzureMI</code></li> <li><code>Attribute.extensionType : mssqlAzureMI</code></li> </ul> <p>For more information, see <a href="#">MSSQL Azure Managed Instance Target Connector CLI Configuration</a>.</p>

### Revised calls in 4.1.1

The following calls were revised in 4.1.1 and these revisions are applicable in all later 4.x releases:

Command	Revision
<code>listPasswordViewRequestSummary</code> <code>listPasswordViewRequestSummaryByRequestor</code>	<p>The returned list of password view requests now includes connection idle timeout values if they are specified.</p>
<code>searchPasswordViewPolicy</code> <code>searchPasswordViewRequestSummary</code> <code>searchPasswordViewRequestSummaryByRequestor</code>	<p>New optional parameter: <code>PasswordViewRequest.connectionTimeout</code> can be used to filter results for requests with connection idle timeouts greater than or equal to the specified value (in minutes). (Useful for identifying extended timeout requests.)</p>

## Revised calls in 4.0

The following calls were revised in 4.0 and these revisions are applicable in all later 4.x releases:

Command	Revision
viewAccountPassword	New optional parameter: <code>PasswordViewRequest.comments</code> which specifies comments to be added to the view password request.
addPasswordPolicy updatePasswordPolicy	New optional parameters: <ul style="list-style-type: none"> <li>• <code>Attribute.disallowSameClassRepeat=boolean</code></li> <li>• <code>Attribute.maxClassRepeat=numeric</code></li> </ul>
addPasswordViewPolicy updatePasswordViewPolicy	New optional parameter: <code>PasswordViewPolicy.passwordViewRequestBanner</code> which defines banner text to be displayed on the Password View Policy.

## Access Free PAM Training Videos From the IMS Software Academy

The Broadcom Identity Management Security division **IMS Software Academy** provides free education videos to help you get the most out of your IMS products.

Visit the [IMS Software Academy](#), create your account, and get started today.

### Access the IMS Software Academy

To access the free education videos, open the [IMS Software Academy](#) in a browser, then do one of the following steps to access the content:

- Log in using your existing Broadcom credentials.
- If you do not have Broadcom credentials, register by providing your corporate email address.

Once logged in, the **Dashboard** page opens, as shown in the following screen capture:

The screenshot displays the IMS Software Academy dashboard. At the top, there is a search bar labeled "Search for enrolled courses" and a "Dashboard" button. Below the header, a banner features logos for IMS Software Academy, Broadcom Software, Symantec VIP, Symantec PAM, Symantec SiteMinder, and Layer7 API Management. The main content area is divided into two columns. The left column shows "Total Number of Courses" with 4 Enrolled Courses and 0 Completed Courses, and a "Recent Activity" section listing three enrollments in Layer7 API Management courses. The right column displays two course cards: "Symantec VIP Authentication Hub Basics" (2 Modules, 0% progress) and "Layer7 API Management Basics" (10 Modules, 0% progress).

### Locate the PAM Courses

If you know the specific name of a course, enter it in the **Search Catalog** field at the top of the screen. Otherwise, do the following steps to access the PAM catalog:

1. Select the **Dashboard** button in the top left.
2. Select the **Catalog** entry from the drop-down menu that appears.
3. Select the **Privileged Access Manager (PAM)** entry from the **Category** drop-down menu.
4. Select **Apply**.
5. The PAM course catalog opens, displaying the newest five courses. To access previous courses, use

the page selector  at the bottom of the course list.

### Available PAM Courses

The following Privileged Access Manager courses are currently publicly available:

- **Symantec PAM Competency - Threat Analytics:** The modules in this course describe how to integrate Symantec PAM and Symantec Threat Analytics to evaluate the risk of privileged user activity to detect and mitigate threats from suspicious activity.
- **Symantec PAM Competency - PAM Server Control:** The modules in this course provide a complete foundational understanding of the integrated PAM Server Control module, which provides host-based security for your most sensitive physical, virtual, or cloud-based systems.
- **Symantec PAM Competency - Architecture:** The modules in this course describe the core PAM architecture and also that of PAM Utility Appliances, which are required to support PAM Server Control.
- **Symantec PAM Basics:** The modules in this course cover a wide range of foundational information, including overviews of essential Symantec PAM concepts, upgrade best practices, and how to plan and implement a high-availability PAM cluster.
- **Symantec PAM - What's New in Symantec PAM 4.0:** This video provides a brief overview of Symantec PAM followed by presentations and demos of the new features in version 4.0.
- **Symantec PAM - Tech Talk: Mitigating Against the Pwnkit Vulnerability:** This Tech Talk discusses how to mitigate the threat of the Pwnkit vulnerability.
- **Symantec PAM - Secrets Management Overview:** This course provides an Overview and Demo of the Secrets Management functionality that was introduced in PAM 4.1.
- **Symantec PAM - Secrets Management Secret Types:** This course provides an overview of the types of secrets that are managed by the secrets management functionality that was introduced in PAM 4.1.
- **Symantec PAM - April Tech Talk - Secrets Management:** This Tech Talk delves deeper into the PAM secrets management functionality.

Not seeing any courses that interest you? Let us know what you would like to learn more about, and we will add it to the list of potential future offerings.

## Related Products

The following products integrate with Privileged Access Manager but are released independently:

- Socket Filter Agents (SFAs) – To use SFAs, see [Socket Filter Agent Support](#).
- A2A Manager Clients – To use the A2A Client, see [Add and Run Credential Manager A2A Requestors](#).
- Windows Proxy – To use the Windows Proxy, see [Add a Windows Proxy Connector](#) and [How to Install a Windows Proxy for Credential Manager](#).

For information about which Privileged Access Manager releases support these products, see [Supported Environments](#). To download the software, go to the [Download Management](#) page on the Support site. In the top field of the page, start entering "Privileged Access" and then select the product page when it becomes available. The product downloads become available.

### NOTE

#### Support Site Notes:

- For the A2A Client, the software is named **Privileged App to App Manager**.
- For the Windows Proxy, the software is under Privileged Access Manager - DEBIAN and under Privileged Access Manager Credential Manager - DEBIAN.



## Upgrading

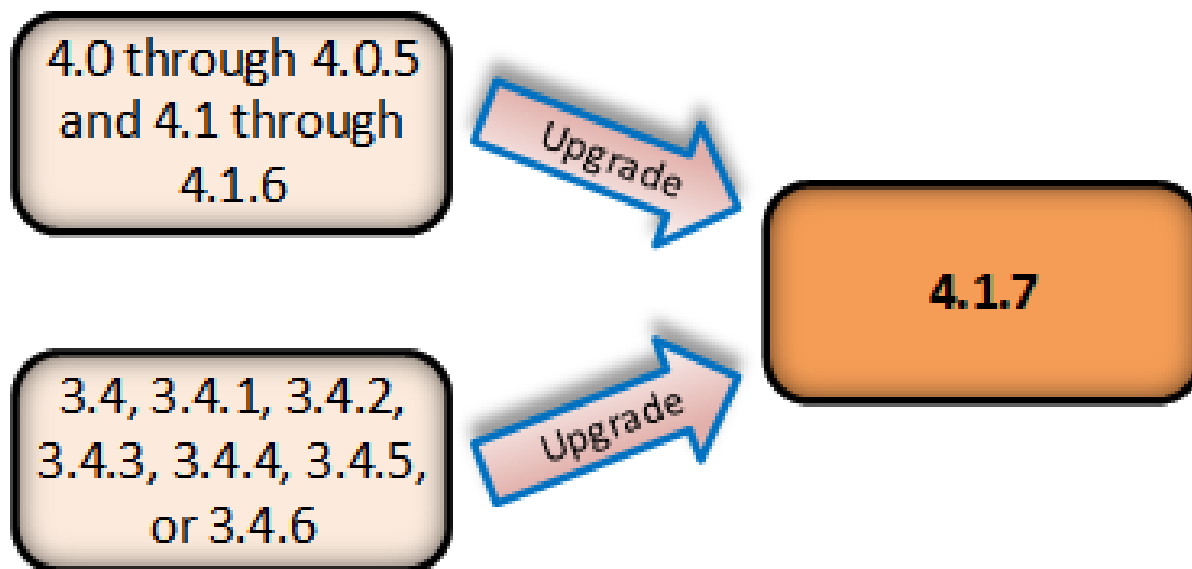
You can upgrade directly to PAM 4.1.7 from existing environments running the following release versions:

- **3.4.x:** 3.4, 3.4.1, 3.4.2, or 3.4.3, 3.4.4, 3.4.5, or 3.4.6.
- **4.0.x:** 4.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, or 4.1.6.

### NOTE

To upgrade from a 3.3.x environment, first upgrade to 4.0. For more information, see the [4.0 upgrade documentation](#).

The supported direct upgrade paths are illustrated in the following diagram:



### TIP

We recommend that you test the upgrade in a non-production environment before you upgrade your production environment.

**To upgrade successfully, do the following procedures:**

### NOTE

If your PAM environment is deployed as a multisite cluster, refer to [Upgrading Across a Multi-Site Cluster](#) before you begin the upgrade process.

1. Complete the [Upgrade Prerequisites](#).
2. Use the appropriate procedure to upgrade your PAM server or servers:
  - [Upgrade a Single Appliance to 4.1.7](#)
  - [Upgrade Appliances in a Cluster to 4.1.7](#)
3. If you have deployed PAM SC, [upgrade your PAM SC Utility Appliances](#)
4. Upgrade auxiliary components, as applicable:
  - [Upgrade a Socket Filter Agent \(SFA\)](#)
  - [Upgrade a Credential Manager A2A Client](#)
  - Upgrade a Windows Proxy ([uninstall the old Windows Proxy software](#), then [install the new version](#))
5. If you have deployed PAM SC, upgrade the following components:

- [PAM SC Utility Appliances](#)
- [PAM SC Endpoints](#)

### **Upgrades and FIPS Mode Operation**

If PAM is already operating in FIPS mode, the PAM server remains in FIPS mode when you upgrade to a newer release. Any upgrade-related cryptographic changes that relate to FIPS mode compliance will be clearly stated in this topic and in the Release Information section.

To move from commercial (Non-FIPS) to FIPS mode operation, you must make changes to licensed products. Please contact your assigned Account Director for more details.

## **Upgrade Prerequisites for 4.1.7**

Complete the following upgrade prerequisites before starting the upgrade to 4.1.7:

### **Verify That Your Environment Is Running a Supported Version In the Upgrade Path**

Verify that your environment is running one of the following releases that are supported for direct upgrade to 4.1.7:

- 3.4, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, or 3.4.6
- 4.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, or 4.1.6.

#### **NOTE**

For more information about upgrade paths, see [Upgrading](#).

### **Review Minimum Free Space**

Ensure that your hard drive has **at least 16 GB of space available** (64 GB recommended) to upload, decompress, and install the new release. Two seemingly unrelated errors can be caused by insufficient disk space:

- PAM-CMN-1344: Problem applying the upgrade package. Details: Error verifying the authenticity of the upgrade package! This error occurs because there is not enough space to decrypt the encrypted upgrade file.
- PAM-CMN-3349: Cannot upgrade because patch is not HMAC signed. This error occurs because there is not enough space to extract required files after decryption.

### **Back Up Your Privileged Access Manager Appliance**

Before you upgrade a Privileged Access Manager appliance, create a backup of your appliance instance. If the upgrade is unsuccessful, you can revert to the backup.

#### **WARNING**

Back up your appliance, even if you backed it up before a previous upgrade.

Depending on the type of appliance you have, follow the relevant guidelines:

- **Privileged Access Manager Hardware appliances:** The upgrade procedure backs up a hardware appliance to its second hard drive before initiating the upgrade. No action is required at this time. For more information, see [Upgrade a Single Appliance to 4.1.7](#).
- **VMware appliances:** Take a snapshot of the VMware OVA. For specific instructions on creating a snapshot of an OVA, see the [VMware documentation](#).
- **AWS AMI appliances:** Take a snapshot of the AMI instance. For specific instructions on backing up an AMI instance, see the [AWS documentation](#).
- **Azure VM appliances:** Take a snapshot of the VM instance. For specific instructions on backing up an Azure instance, see the [Azure documentation](#).

If you take a snapshot while the instance is operating, the snapshot can take a long time to complete. To save time and storage media, shut down the instance and then take the snapshot.

### **Put Your Appliance Into Maintenance Mode**

Put your appliance into [Maintenance Mode](#) before initiating the upgrade.

### **Prepare the Hardware Appliance**

When upgrading a physical appliance, Privileged Access Manager copies the primary drive data (including database and configuration files) onto its backup drive before applying the update. If there is any issue with the upgrade, you can restore your appliance to its preupgrade state from the backup.

If an upgrade error occurs, follow the instructions in [Recover the Hardware Appliance](#).

### **Ensure Clustering Ports are Open**

If you are upgrading a cluster, ensure that ports 3307, 13307, and 8443 are open. These ports are required for the enhanced clustering in this release. See [Cluster Deployment Requirements](#) for more information.

### **Review Strong Cryptography on Cisco and UNIX Target Connectors**

Release 4.1.7. supports the latest recommended strong cryptography for secure SSH communications in Cisco and UNIX target connectors. All target servers must support at least one of the security algorithms from each of the following categories:

Privileged Access Manager 4.1.7 supports the following algorithms:

<b>Cryptographic Algorithms</b>	<b>Non-FIPS mode Supported List</b>	<b>FIPS mode Supported List</b>	<b>Deprecated algorithms*</b>
Cipher	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes128-cbc</li> <li>• aes256-cbc</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com,</li> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes128-cbc</li> <li>• aes256-cbc</li> </ul>	<ul style="list-style-type: none"> <li>• aes192-ctr</li> <li>• aes192-cbc</li> <li>• 3des-ctr</li> <li>• 3des-cbc</li> <li>• blowfish-cbc</li> <li>• arcfour256</li> <li>• arcfour128</li> <li>• arcfour</li> </ul>
Key Exchange	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• curve25519-sha256@libssh.org</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group-exchange-sha256</li> </ul>	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group-exchange-sha256</li> </ul>	<ul style="list-style-type: none"> <li>• diffie-hellman-group14-sha1, diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1</li> </ul>

Cryptographic Algorithms	Non-FIPS mode Supported List	FIPS mode Supported List	Deprecated algorithms*
Hash	<ul style="list-style-type: none"> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• hmac-sha1-etm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• hmac-sha1-etm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha1</li> <li>• hmac-sha1-96</li> <li>• hmac-md5-96</li> <li>• hmac-md5</li> </ul>
Server Host Key	<ul style="list-style-type: none"> <li>• ssh-ed25519</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-512</li> <li>• rsa-sha2-256</li> </ul>	<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-512</li> <li>• rsa-sha2-256</li> </ul>	<ul style="list-style-type: none"> <li>• ssh-rsa</li> <li>• ssh-dss</li> </ul>
Compression	<ul style="list-style-type: none"> <li>• none</li> </ul>	<ul style="list-style-type: none"> <li>• none</li> </ul>	

\**Deprecated algorithms* will continue working in PAM to support backward compatibility. Using newer and more secure algorithms is recommended.

You can disable the deprecated algorithms on the SSH-2 tab of the UNIX or Cisco target application configuration. For more information, go to [Add a UNIX Target Connector](#). Read the instructions for the SSH-2 Tabs - Cipher, Hash, Key Exchange, Compression, Server Host Key.

### Review Strong Cryptography for Access Management - SSH Proxy and SSH MindTerm

Release 4.1.7 supports the latest recommended strong cryptography for more secure SSH communications for Access Management using SSH Proxy and SSH Mindterm. These algorithms are listed in the PAM UI under **Configuration, Security, Cryptography**. All target servers must support at least one of the cryptographic algorithms from each of the algorithm sections. PAM has three lists (also called categories or sets) of cryptographic algorithms:

- **Supported:** All the algorithms supported by PAM. This list appears in the PAM UI on Cryptographic pages when you select the eye icon next to every algorithm.
- **Recommended:** All the algorithms that PAM strongly recommends customers to use. PAM, by default, only uses the algorithms from the "recommended" list. This list is also used when "Use Default" is checked.
- **Allowed/customized:** By default, this is a recommended list. This list is a customized version of algorithms specified by end users in the PAM UI.

PAM 4.1.7 uses the following list of algorithms:

SSH Proxy Cryptographic Algorithms				
Cryptographic Algorithms	Non-FIPS mode Supported List	Non-FIPS mode Recommended List	FIPS mode Supported List	FIPS mode Recommended List
Cipher	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• chacha20-poly1305@openssh.com</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• chacha20-poly1305@openssh.com</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• chacha20-poly1305@openssh.com</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• chacha20-poly1305@openssh.com</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> </ul>

Key Exchange	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group1-sha1</li> <li>• diffie-hellman-group-exchange-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group14-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group14-sha1</li> <li>• curve25519-sha256</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group1-sha1</li> <li>• diffie-hellman-group-exchange-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• e</li> <li>• e</li> <li>• e</li> <li>• e</li> <li>• e</li> </ul>
Hash	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• umac-128@openssh.com</li> <li>• umac-64-etm@openssh.com</li> <li>• umac-64@openssh.com</li> <li>• hmac-sha1</li> <li>• hmac-md5-96</li> <li>• hmac-md5</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• umac-128@openssh.com</li> <li>• umac-64-etm@openssh.com</li> <li>• umac-64@openssh.com</li> <li>• hmac-sha1</li> <li>• hmac-md5-96</li> <li>• hmac-md5</li> </ul>	<ul style="list-style-type: none"> <li>• h</li> <li>• h</li> <li>• h</li> <li>• e</li> <li>• u</li> <li>• e</li> <li>• h</li> <li>• e</li> </ul>
Server Host Key	<ul style="list-style-type: none"> <li>• ssh-ed25519</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-256</li> <li>• rsa-sha2-512</li> <li>• ssh-rsa</li> </ul>	<ul style="list-style-type: none"> <li>• ssh-ed25519</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• ssh-rsa</li> </ul>	<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-256</li> <li>• rsa-sha2-512</li> <li>• ssh-rsa</li> <li>• ssh-ed25519</li> </ul>	<ul style="list-style-type: none"> <li>• e</li> <li>• e</li> <li>• e</li> <li>• e</li> <li>• s</li> </ul>
Compression	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• n</li> <li>• z</li> <li>• z</li> </ul>

**SSH Mindterm Cryptographic Algorithms**

Cryptographic Algorithms	Non-FIPS mode Supported List	Non-FIPS mode Recommended List	FIPS mode Supported List	FIPS Reco
--------------------------	---------------------------------	-----------------------------------	-----------------------------	--------------

Cipher	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes256-cbc</li> <li>• aes192-cbc</li> <li>• 3des-ctr</li> <li>• 3des-cbc</li> <li>• blowfish-cbc</li> <li>• blowfish-ctr</li> <li>• arcfour256</li> <li>• arcfour128</li> <li>• arcfour</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes256-cbc</li> <li>• aes192-cbc</li> </ul>	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes256-cbc</li> <li>• aes192-cbc</li> <li>• 3des-ctr</li> <li>• 3des-cbc</li> <li>• blowfish-cbc</li> <li>• blowfish-ctr</li> <li>• arcfour256</li> <li>• arcfour128</li> <li>• arcfour</li> </ul>	<ul style="list-style-type: none"> <li>• a</li> <li>• a</li> <li>• a</li> <li>• a</li> <li>• a</li> <li>• a</li> </ul>
Key Exchange	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group1-sha1</li> <li>• diffie-hellman-group-exchange-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group14-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group14-sha256</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group18-sha512</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group1-sha1</li> <li>• diffie-hellman-group-exchange-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• e</li> <li>• e</li> <li>• e</li> <li>• d</li> <li>• s</li> <li>• d</li> </ul>
Hash	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha512@ssh.com</li> <li>• hmac-sha256@ssh.com</li> <li>• hmac-sha256-2@ssh.com</li> <li>• hmac-sha1</li> <li>• hmac-sha1-96</li> <li>• hmac-md5-96</li> <li>• hmac-md5</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha512@ssh.com</li> <li>• hmac-sha256@ssh.com</li> <li>• hmac-sha256-2@ssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• hmac-sha512@ssh.com</li> <li>• hmac-sha256@ssh.com</li> <li>• hmac-sha256-2@ssh.com</li> <li>• hmac-sha1</li> <li>• hmac-sha1-96</li> <li>• hmac-md5-96</li> <li>• hmac-md5</li> </ul>	<ul style="list-style-type: none"> <li>• h</li> <li>• h</li> <li>• h</li> <li>• h</li> <li>• h</li> <li>• h</li> </ul>
Server Host Key	<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-256</li> <li>• rsa-sha2-512</li> <li>• ssh-rsa</li> <li>• ssh-dss</li> </ul>	<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• ssh-rsa</li> </ul>	<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• rsa-sha2-256</li> <li>• rsa-sha2-512</li> <li>• ssh-rsa</li> <li>• ssh-ds</li> </ul>	<ul style="list-style-type: none"> <li>• e</li> <li>• e</li> <li>• e</li> <li>• s</li> </ul>
Compression	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• none</li> <li>• zlib@openssh.com</li> <li>• zlib</li> </ul>	<ul style="list-style-type: none"> <li>• n</li> <li>• z</li> <li>• z</li> </ul>

**NOTE**  
**Next Step:**

- [Upgrade a Single Appliance to 4.1.7](#)  
or
- [Upgrade Appliances in a Cluster to 4.1.7](#)

## Upgrade a Single Appliance to 4.1.7

This content describes how to upgrade the PAM software to 4.1.7 on a *single* hardware or virtual appliance.

### NOTE

To upgrade a clustered appliance, see [Upgrade Appliances in a Cluster to 4.1.7](#).

Allow sufficient time to upgrade. The process takes some time to complete because it backs up your previous software, configuration, and provisioning database. Do not interrupt it.

### Review the Upgrade Prerequisites

Before you upgrade, [review the prerequisites](#) and verify that they have been met.

### Download the Patch

Download the software for this release from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

### Prepare for the Upgrade

Complete this procedure before starting the upgrade.

#### Follow these steps:

1. Confirm that all [prerequisites](#) are completed.
2. Log in to the PAM UI as a Configuration Manager or Global Administrator. You must have privileges to modify Configuration options and Global Settings.
3. To prevent users from logging in during the upgrade, turn on **Maintenance Mode** from **Configuration, Diagnostics, System**.
4. If your installation uses an NFS, CIFS, or Amazon S3 mount to store session recordings, ensure that the mount is up:
  - a. Navigate to **Configuration, Logs, Session Recording**.
  - b. Select the **External Storage** tab.
  - c. In the **Primary Mount Settings** section, confirm that **Mount Status** states "mounted".

After you are finished with this procedure, perform the upgrade.

### Perform the Upgrade

After you prepare for the upgrade, apply the upgrade patch.

#### Follow these steps:

1. From the PAM UI, navigate to **Configuration, Upgrade**.
2. In the **Upgrade History** section, confirm that the installed upgrades include any necessary patches to upgrade to the current release. For more information about the necessary patches, see [Upgrading](#).
3. Select **Choose File** and browse to the **CAPAM\_4.1.7.p.bin** file.
4. Select **Upload and Apply** to apply the patch automatically after the file uploads, or select **Upload** and **Apply** separately. The upgrade begins.

### NOTE

#### Appliance Backups:

Manually backup virtual appliances *before* performing the upgrade (see [Upgrade Prerequisites](#)).

Hardware appliances are backed up automatically during the upgrade process according to their model and current PAM version:

- On a 304L hardware appliance, the upgrade procedure automatically performs a full backup (to its second hard drive) before initiating the upgrade.
- On a 404L hardware appliance, *if you are upgrading from 4.1.1*, the upgrade procedure asks you if you want to perform a full backup before initiating the upgrade process. If you are upgrading from any other version, the upgrade procedure automatically performs a full backup before initiating the upgrade process. (The same as on the 304L appliance.)

### **WARNING**

Depending on the size of your database, the upgrade might take a long time to complete. Keep your browser open until you see a reboot message. Do not interrupt the upgrade process.

5. After the upgrade is complete, a dialog appears. Select **OK** to reboot the appliance.

### **IMPORTANT**

If you are running the upgrade procedure using the PAM Client, you must terminate it while the PAM server reboots so that it will update itself to the new version when you start it again after the upgrade is complete. Follow these steps:

1. When a dialog stating "Your session connection is lost. The session will be terminated. Re-login to continue" select the **OK** button.
2. To terminate the PAM Client, select the **X** button in the upper right corner of the next screen.
3. Proceed to Step 6.

### **TIP**

If the reboot message still appears in the PAM UI or the LCD display (hardware appliance) after 5 minutes, continue to Step 6.

6. When the reboot is complete, log back in to the PAM UI. If you are using the PAM Client, wait while it updates itself to the new PAM version.

### **NOTE**

If you cannot initially log in, wait from 15 to 30 minutes and try again.

7. Review the following items to confirm that the upgrade is successful:
  - The **Upgrade History** section shows the correct file name, with the current time and date.
  - The correct release number is shown in the **Version** field on the **System Info** pane.
8. Continue to complete any post upgrade procedures.

## **Post Upgrade Procedures**

After the upgrade completes successfully, complete the relevant post-upgrade tasks:

- [Clear the Browser and JRE caches](#)
- [Update the Credential Manager Remote CLI and Java API](#)
- [Verify OCS Smart Card for Entrust nShield HSM is Installed](#)
- [Change the Login Timeout](#)

### **WARNING**

If you turned on Maintenance Mode, turn it off after you complete the post-upgrade tasks.

### ***Clear Browser and JRE Caches***

Instruct users who connect to the PAM appliance through a web browser to clear their browser and JRE caches before they log in again. Communicate this instruction to administrators *and* standard users.



**Follow these steps:**

1. For each browser that you use to access Privileged Access Manager, clear its cache, and close it.
2. Clear the Java cache in the Java JRE.
3. Restart the browser.

If you do not clear the Java cache, the following error message appears on the Access page:

The Access page failed to load. Please verify that Java is installed and is enabled in your browser, and that the Next-generation Java Plug-in is enabled. If so, then the download of the Java applet might be taking too long. Please try again. If the problem persists, please contact your administrator.

**Update the Credential Manager Remote CLI and Java API**

If you use the Remote CLI or Java API to manage Credential Manager, update to the 4.1.7 version of RemoteCLI zip on your designated client system. For more information, see [Install and Set Up the Remote CLI and Java API](#).

**Verify That the OCS Smart Card for Entrust nShield HSM is Installed**

On the hardware appliance or a VMware OVA, the Credential Manager can work with an Entrust nShield HSM for hardware encryption.

After you upgrade, ensure that the OCS smart card for the HSM is inserted into the Entrust nShield HSM.

The smart card is necessary in the following situations:

- Before you reboot PAM
- Before you restart a cluster
- After you apply a patch

After PAM is successfully communicating with the HSM, you can remove the card.

**Revert the Login Timeout**

If you changed the Login Timeout before doing the upgrade, change it back to your preferred setting. Navigate to **Settings, Global Settings** and set the **Login Timeout**.

## Upgrade Appliances in a Cluster to 4.1.7

This content describes how to upgrade the PAM software on all cluster members without removing them from the cluster. This method is the simplest, but it keeps your cluster offline for the longest amount of time. If minimal downtime is a priority for your environment, see [Migrating Across a Multi-Site Cluster](#) for alternative methods to upgrade a cluster.

To upgrade the software on all the appliances in a cluster, follow these instructions:

**NOTE**

To upgrade a single (unclustered) appliance, see [Upgrade a Single Appliance to 4.1.7](#).

**Review the Upgrade Prerequisites**

Before you upgrade, [review the prerequisites](#).

**Download the Patch**

Download the software for this release from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

## Prepare Cluster Members for the Upgrade

Complete the following procedure on *each member* of the cluster before starting the upgrade.

### Follow these steps:

1. Confirm that all appliances are running the same release version and have the same patch set. To verify this information, navigate to **Configuration, Upgrade**, and review the Upgrade History.

#### WARNING

If the appliances in the cluster are a mix of releases or patch sets, upgrade each mismatched appliance to the same release and patch set. Ensure that the version you upgrade to supports an upgrade to the latest release (see [Upgrading](#)). If the release and patch match but they are not at a version that can be upgraded, contact CA Support for instructions.

2. Confirm that all [prerequisites](#) are completed.
3. Log in to the PAM UI as a Configuration Manager or Global Administrator. You must have privileges to modify Configuration options and Global Settings.
4. To prevent user from logging in during the upgrade, turn on **Maintenance Mode** from **Configuration, Diagnostics, System**.
5. If your installation uses an NFS, CIFS, or Amazon S3 mount to store session recordings, ensure that the mount is up:
  - a. Navigate to **Configuration, Logs, Session Recording**.
  - b. Select the **External Storage** tab.
  - c. In the **Primary Mount Settings** section, confirm that **Mount Status** states "mounted".

After you are done preparing, perform the upgrade.

## Perform the Upgrade

The following procedure is the simplest method to upgrade a cluster, but the cluster is down for the longest amount of time. If limiting downtime is a priority over simplicity, go to [Migrating Across a Multi-Site Cluster](#) to learn about an alternative upgrade method.

#### NOTE

We recommend using the PAM UI in a web browser to upgrade the Privileged Access Manager appliance.

### Follow these steps:

1. If clustering is active, turn it off at any of the cluster members.  
**To turn off the cluster:**
  - a. Log in as an administrator with configuration privileges (for example, "config" or "super").
  - b. Navigate to **Configuration, Clustering**, and select the **Cluster Status** tab.
  - c. Select **Turn Cluster Off** at the bottom of the page. Wait until a notification indicates that synchronization is off.
2. At the cluster member to be upgraded:
  - a. Navigate to **Configuration, Upgrade**.
  - b. In the **Upgrade History** section, confirm that your installed upgrades include all necessary patches for upgrading to the current release. See [Upgrading](#) for more information.
  - c. Select **Choose File** and browse to the **CAPAM\_4.1.7.p.bin** file.
  - d. Select **Upload and Apply** to apply the upgrade automatically after the file uploads, or select **Upload** and **Apply** separately. The upgrade begins.

#### NOTE

#### Appliance Backups:

Manually backup virtual appliances *before* performing the upgrade (see [Upgrade Prerequisites](#)).

Hardware appliances are backed up automatically during the upgrade process according to their model and current PAM version:

- On a 304L hardware appliance, the upgrade procedure automatically performs a full backup (to its second hard drive) before initiating the upgrade.
- On a 404L hardware appliance, *if you are upgrading from 4.1.1*, the upgrade procedure asks you if you want to perform a full backup before initiating the upgrade process. If you are upgrading from any other version, the upgrade procedure automatically performs a full backup before initiating the upgrade process. (The same as on the 304L appliance.)

**WARNING**

Depending on the size of your database, the upgrade might take a long time to complete. Keep your browser open until you see a reboot message. Do not interrupt the upgrade process.

- e. After the upgrade is complete, a dialog appears. Select **OK** to reboot the appliance.

**IMPORTANT**

If you are running the upgrade procedure using the PAM Client, you must terminate it while the PAM server reboots so that it will update itself to the new version when you start it again after the upgrade is complete. Follow these steps:

1. When a dialog stating "Your session connection is lost. The session will be terminated. Re-login to continue" select the **OK** button.
2. To terminate the PAM Client, select the **X** button in the upper right corner of the next screen.
3. Proceed to Step f.

**TIP**

If the reboot message still appears in the PAM UI or the LCD display (hardware appliance) after 5 minutes, continue to Step f.

- f. When the reboot is complete, log back in to the PAM UI. If you are using the PAM Client, wait while it updates itself to the new PAM version.

**NOTE**

If you cannot initially log in, wait from 15 to 30 minutes and try again.

- g. Review the following items to confirm that the upgrade is successful:
- The **Upgrade History** section shows the correct file name, with the current time and date.
  - The correct release number is shown in the **Version** field on the **System Info** pane.

3. Repeat step 2 for every cluster member.

**WARNING**

**SailPoint Users Note:** If you have integrated a SailPoint database in PAM before this upgrade, follow these steps:

- The server that previously had the SailPoint integration must be specified as the first member of the primary site cluster.
- The cluster must be turned on from that cluster member.

Failure to follow these steps results in a total loss of the PAM SailPoint database. This loss happens because the first member of the primary site is the database initialization source when you turn on a cluster. If the SailPoint database exists only on another member, it is overwritten. Beginning with version 3.3.1, the SailPoint database is replicated to all members, so this step is unnecessary when upgrading to subsequent versions.

4. On the *primary cluster member*, turn clustering back on:
- a. Log in to the primary member and confirm that all data is restored.
  - b. Navigate to **Configuration, Clustering**.
  - c. Select **Turn Cluster On** at the bottom of the page. Wait approximately 5 minutes until Status indicates that clustering is now on.
5. Complete any required [post-upgrade procedures](#).

## Post Upgrade Procedures

After the upgrade completes successfully, complete the relevant post-upgrade tasks:

- [Clear the Browser and JRE caches](#)
- [Update the Credential Manager Remote CLI and Java API](#)
- [Verify OCS Smart Card for Entrust nShield HSM is Installed](#)
- [Change the Login Timeout](#)

### WARNING

Important! If you turned on Maintenance Mode, turn it off after you complete the post-upgrade tasks.

### **Clear Browser and JRE Caches**

Instruct all users who connect to Privileged Access Manager through a web browser to clear their browser and JRE caches before they log in again. Communicate this instruction to administrators *and* standard users.

### **Follow these steps:**

1. For each browser that you use to access Privileged Access Manager, clear its cache, and close it.
2. Clear the Java cache in the Java JRE.
3. Restart the browser.

If you do not clear the Java cache, the following error message appears on the Access page:

The Access page failed to load. Please verify that Java is installed and is enabled in your browser, and that the Next-generation Java Plug-in is enabled. If so, then the download of the Java applet might be taking too long. Please try again. If the problem persists, please contact your administrator.

### **Update the Credential Manager Remote CLI and Java API**

If you use the Remote CLI or Java API to manage Credential Manager, update to the 4.1.7 version of `RemoteCLI` zip on your designated client system. For more information, see [Install and Set Up the Remote CLI and Java API](#).

### **Verify OCS Smart Card for Entrust nShield HSM is Installed**

On the hardware appliance or a VMware OVA, the Credential Manager can work with a Entrust nShield HSM for hardware encryption.

After you upgrade, ensure that the OCS smart card for the HSM is inserted into the Entrust nShield HSM.

The smart card is necessary in the following situations:

- Before you reboot PAM
- Before you restart a cluster
- After you apply a patch

After PAM is successfully communicating with the HSM, you can remove the card.

### **Change the Login Timeout**

If you changed the Login Timeout before doing the upgrade, change it back to your preferred setting. Navigate to **Settings, Global Settings** and set the **Login Timeout**.

## Upgrading Across a Multi-Site Cluster

Upgrade strategies differ depending on your priorities. Consider whether you want to minimize the complexity of the upgrade, or minimize cluster downtime. These priorities can determine the upgrade method.

**TIP**

Cluster configurations and requirements can vary considerably. To discuss your upgrade options, contact Broadcom Support.

Some of the methods for upgrading a multi-site cluster are described in the following topics:

Regardless of which method you use, remember these guidelines:

- Always back up your data before upgrading
- Do not run mixed PAM release versions in a cluster.
- Be mindful not to lose any data. The database of the primary member in the primary site holds the data. This database gets replicated. Any changes to a member outside of a live cluster can break cluster synchronization. For example, exercising an access method which changes the password on a target device breaks synchronization.
- The upgrade takes a long time to complete. To allow time to upload and upgrade, remove the timeout. Navigate to **Settings, Global Settings** and set the **Login Timeout** to 0. Log out and log back in to ensure the change.

**Upgrade Method to Limit Downtime**

This section explains *one* upgrade method. The goal of this phased upgrade is to limit how long the cluster is off line. This method is not the only way to upgrade a cluster.

**WARNING**

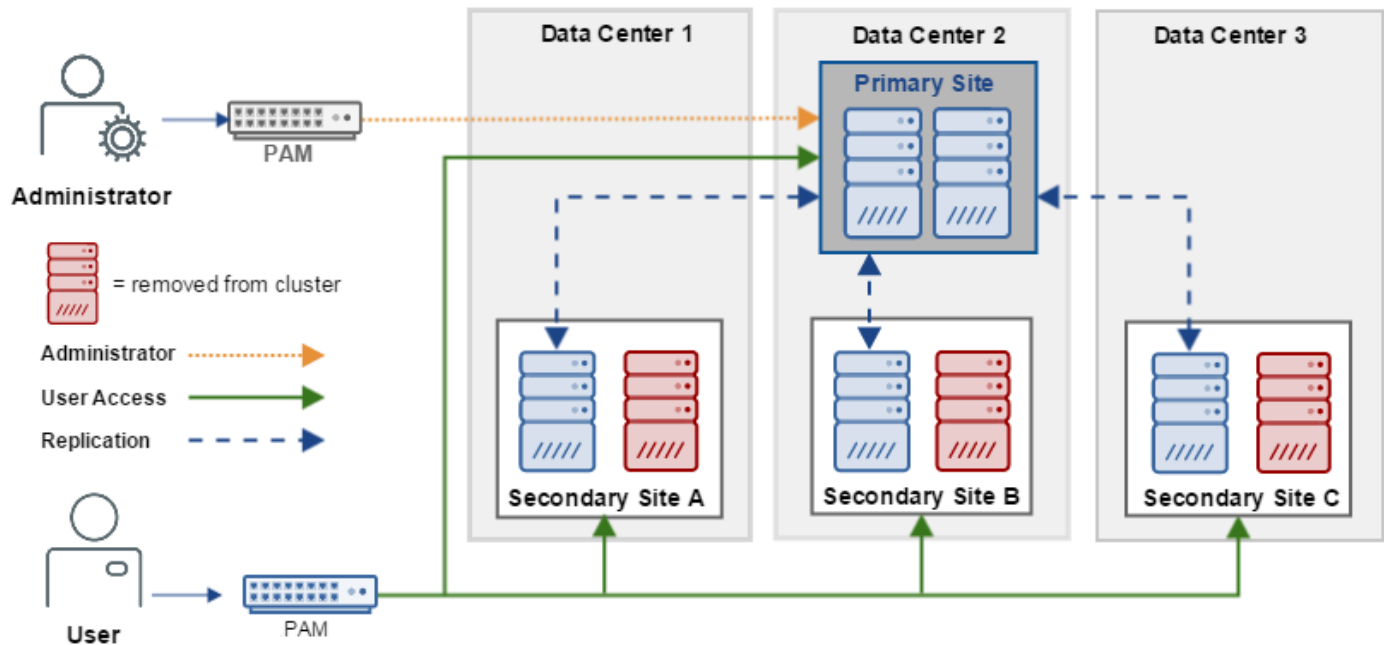
This phased upgrade is a guideline. This process is not intended as the sole resource for upgrading a multi-site cluster to limit downtime. You might have other processes and resources, such as runbooks, that are specific for your infrastructure. Use those resources together with this phased procedure.

The following phases explain the upgrade flow of a multi-site cluster across several data centers.

***Phase One***

The following graphic illustrates the following steps:

1. Remove all secondary members except one from the cluster at each secondary site. The picture shows one of the two secondary members at each secondary site that is removed from the cluster. The red systems represent removed members.  
The capacity of the cluster is reduced but no outage occurs.
2. Upgrade each removed cluster member to the current release.  
You can observe how long it takes to upgrade each member to estimate the upgrading of the entire cluster.

**Figure 5: Phase 1 Cluster Migration****Phase Two**

The second phase reflects a full outage of the cluster. The intention of this phase is to allow only the administrator access to cluster members, not users.

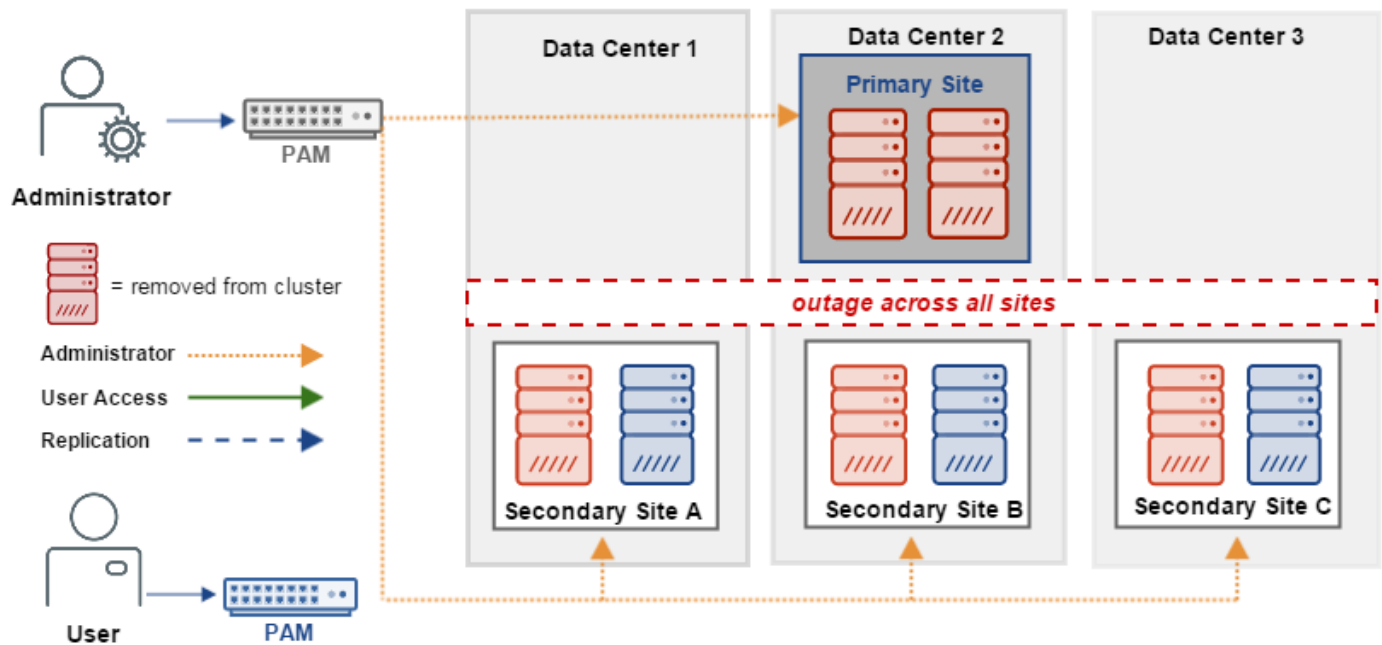
The following graphic reflects the results of these steps:

3. Turn off the cluster.
4. Upgrade the primary members to the current release. In the cluster configuration, list the upgraded primary member first in the list of members.  
You do not have to remove the primary members from the cluster configuration.
5. At the primary site, add back the already upgraded secondary site members.

**TIP**

In a multi-site deployment, operation can resume after adding back only one upgraded node from *each* secondary site. After you turn on the cluster, upgrade each remaining member. To add that member back to an active cluster, select **Subscribe to Active Cluster**.

6. While still at the primary site, remove the existing *non-upgraded* secondary site members from the configuration.

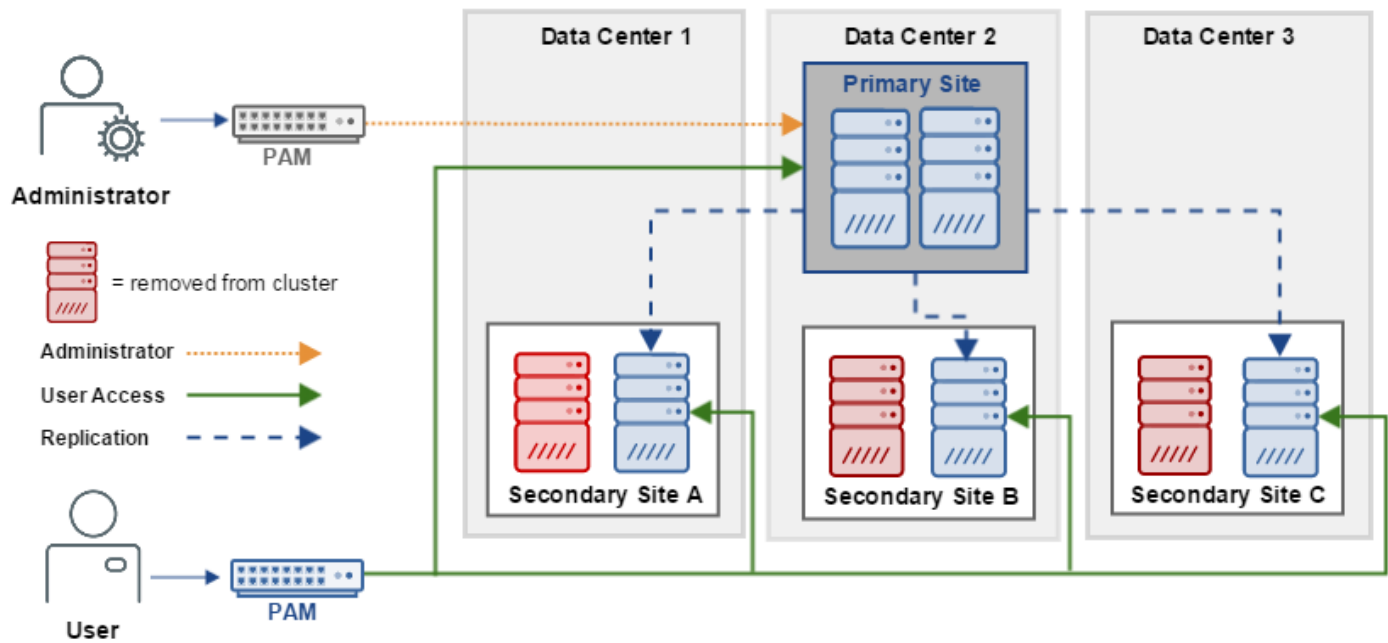
**Figure 6: Phase 2 Cluster Migration****Phase Three**

The third phase brings the upgraded cluster members back online, closing the outage window.

The following graphic shows the phase three steps:

7. Turn on the cluster from the primary member. The primary member is the first one in the list of primary site members.
8. Verify that the primary member data is available across all data centers.

At this point, the cluster is live and users can access resources again.

**Figure 7: Phase 3 Cluster Migration****Phase Four**

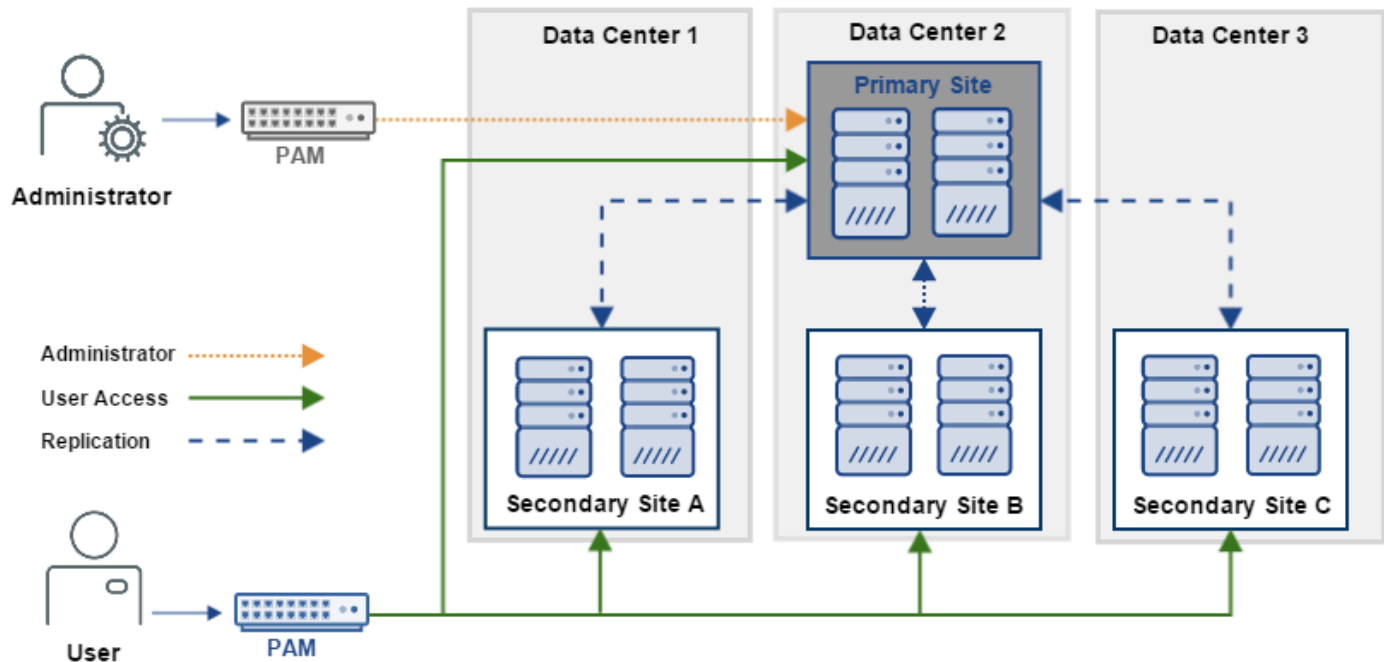
The fourth and final phase brings the remaining secondary members back into the cluster.

The following picture shows the final steps:

9. Upgrade the remaining secondary members to the current release.

10. At each upgraded secondary member, subscribe that member to the active cluster.



**Figure 8: Phase 4 Cluster Migration**

### **Alternative Methods for Upgrading a Multi-Site Cluster**

You might have priorities other than limiting the downtime of your cluster. Consider the following alternative methods for upgrading a multi-site cluster:

- Upgrade each cluster member without removing the member from the cluster.
- Upgrade secondary members then restart the cluster.

#### ***Upgrade Cluster Members Without Removing Them from the Cluster***

**Advantage:** This method is the simplest.

**Disadvantage:** The cluster is offline for the longest timeframe.

#### **Process:**

1. Turn off the cluster.
2. Upgrade all members. You *do not* have to remove the members from the cluster.
3. Turn on the cluster.

#### ***Upgrade Secondary Members Then Restart the Cluster***

##### **NOTE**

This method modifies phase 4 in the previous illustration.

**Advantage:** This method provides a simple way to add upgraded secondary members back into the cluster. An administrator has to change the cluster configuration at the primary site only one time, and not at each new secondary site member.

**Disadvantage:** A brief second outage of the cluster is required.

#### **Process:**

1. Upgrade the secondary members that you removed.

2. Stop the cluster.
3. From a primary site member, add the secondary members back into the cluster.
4. Start the cluster.

### ***Change the Login Timeout***

If you changed the Login Timeout before doing the upgrade, change it back to your preferred setting. Navigate to **Settings, Global Settings** and set the **Login Timeout**.

### **Detailed Upgrade Instructions**

For specific instructions on upgrading cluster members, go to the upgrade instructions for the appropriate release.

## **Upgrade a Socket Filter Agent (SFA)**

This content describes how to upgrade a Socket Filter Agent.

### **Download the Socket Filter Agent Software**

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

### **Upgrade a Linux or UNIX Socket Filter Agent**

Use this procedure to upgrade your Linux or UNIX Socket Filter Agent.

#### **Follow these steps:**

1. Access the computer with the Linux or UNIX SFA to be upgraded. Ensure that the Linux or UNIX SFA is operating.
2. Run the latest Linux or UNIX SFA installer. If you have a pre-existing SFA, the installer updates all files as required. The installer automatically stops the required daemons before the upgrade and restarts them after the upgrade.

### **Upgrade a Windows Socket Filter Agent**

Use this procedure to upgrade your Windows Socket Filter Agent (SFA).

#### **Follow these steps:**

1. Access the computer with the Windows SFA to be upgraded. Ensure that the Windows SFA is operating.
2. Access the Windows Services console and stop the **CA Technologies Socket Filter** service.

#### **NOTE**

The SFA service name is a configurable value. If you have configured a different SFA service name, locate and stop that service name.

3. Uninstall the old Windows SFA.
4. Run the latest Windows SFA installer to install a new SFA.
5. Restart the **CA Technologies Socket Filter** service.

#### **NOTE**

#### **More information:**

- [Install and Configure a Socket Filter Agent](#)

## **Upgrade a Credential Manager A2A Client**

This content describes how to upgrade an existing Credential Manager A2A Client.

## **A2A Client Credential Caching**

The A2A Client maintains the cache *only* in memory. The local storage cache is read only. If there is a power failure, the appliance can recover the cache. If for any reason the appliance is not available, the local storage serves as an alternative cache. For more information about this setting, see [Modify the A2A Client Configuration File](#).

## **Download the A2A Client Software**

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

## **Upgrade the A2A Client on UNIX Systems**

To upgrade an A2A Client on UNIX:

1. Uninstall any existing A2A Client.
2. Install the new A2A Client.
3. Activate the request server.

### **Uninstall the Existing A2A Client on UNIX (Required)**

Before you install a new A2A Client, you must uninstall the existing Client.

#### **WARNING**

If you changed to the default A2A Client configuration file, back up this file.

#### **Follow these steps:**

1. Stop the A2A Client using this command:

```
$CSPM_CLIENT_HOME/cspmclient/bin/cspmclientd stop
```

where `CSPM_CLIENT_HOME` is your installation directory, for example `/opt/catech`

2. Run the uninstall script by entering:

```
$CSPM_CLIENT_HOME/cspmclient/bin/cspmclient_uninstall
```

This script removes all A2A Client directories and files.

3. Reboot the system.

### **Install a New A2A Client on UNIX**

Install and configure the A2A Client on all request servers.

#### **NOTE**

Do not install more than one A2A Client on the same host. If an A2A Client already exists, installing into the same directory overwrites that client.

#### **Follow these steps:**

1. Open a shell command window and navigate to the location of the unzipped A2A Client installation package:

```
cd unzip_location/
```

2. Enter the following commands:

```
chmod u+x setup_unix
```

3. Start the installation script by entering the following command:

```
./setup_unix host_type processor_size cspm_client_home server_address
```

**host\_type:** Specifies the type of UNIX host. Enter `Linux` or `SolarisSparc`

**processor\_size:** Specifies whether to install the 32-bit or 64-bit A2A Client. Enter `32` or `64`.

**cspm\_client\_home:** Names the installation directory for the A2A Client software

*server\_address*: Identifies the IP address or fully qualified domain name (FQDN) of the appliance. If you specify the FQDN, it must match the name in the appliance SSL certificate.

4. If you are upgrading a pre-3.0.1 A2A Client and you want to use local storage caching, enable this caching. Only caching in memory is enabled by default.

Follow these steps:

- a. Navigate to the A2A Client configuration file (*cspm\_client\_config.xml*). The file is in *cspm\_client\_home/catech/cspmclient/config*.
- b. Set the `<preserveCacheBetweenRestarts>` tag to `true`.
- c. Start the A2A Client service by entering: `cspmclientd start`
- d. When prompted, enter a password for local authentication.

### WARNING

Store this password securely. When the `<preserveCacheBetweenRestarts>` tag is set true, the password is required every time the A2A Client is started.

- e. Log in to the PAM UI.
  - f. Navigate to **Credentials, Manage A2A, Clients**.
  - g. Select the A2A Client and select **View** button.
  - h. Select the **Change Key** button.
  - i. Select **Close**.
  - j. Stop the A2A Client service by entering: `cspmclientd stop`
5. Restart the client by entering: `cspmclientd start`

### Activate the Request Server on UNIX

After you install the A2A Client, [activate the request server](#).

### Upgrade the A2A Client on Windows Systems

To upgrade the A2A Client on Windows:

1. Uninstall the existing A2A Client.
2. Install the new A2A Client.
3. Activate the request server.

### Uninstall the Existing A2A Client on Windows (Required)

Before you install a new A2A Client, you must uninstall the existing Client.

### WARNING

If you changed the A2A Client configuration file, back up this file.

Follow these steps:

1. Stop the A2A Client using *one* of the following methods:
  - Use the Windows Services administrative tool and stop the `cspmclientd` service.
  - Open a Command Prompt window and enter: `net stop cspmclientd`
2. Launch the uninstall executable using *one* of the following methods:
  - From the **Control Panel, Programs and Features**, select the **PAM A2A Client**.
  - Navigate to: `%CSPM_CLIENT_HOME%\cspmclient\Uninstall_Password_Authority.CSPM_CLIENT_HOME` is the installation directory, for example, `C:\cspm\cloakware`. Select `Uninstall Password Authority.exe` or `Uninstall PAM A2A Client.exe`. The executable name depends on the existing client version.

The Uninstall window displays.
3. **Select Uninstall.**

When the uninstall finishes, the **Uninstall Complete** window displays. You might need to remove files manually. If so, the uninstaller identifies the files that you must remove.

4. Select **Done**.
5. Reboot the system.

### **Install a New A2A Client on Windows**

Install and configure the A2A Client on all request servers. Installation of more than one A2A Client on the same host is not supported. If an A2A Client already exists in a directory, installing into the same directory overwrites that client.

When you execute the installation from an account that contains special characters, the installation wizard fails. To avoid this problem, right-click the executable file and select **Run As**. The **Run As** dialog opens and prompts for an alternate username and password to use for the installation. Specify the account credentials and continue with the installation.

#### **Follow these steps:**

1. Unzip the installation package.
2. Open a Command window and navigate to the `clients\win` subdirectory.
3. Start the installation wizard by entering `setup_windows32_java.exe` or `setup_windows64_java.exe`. The installation begins.
4. In the **Introduction** window, select **Next**.
5. In the **Choose Install Folder** window, enter, or select the folder where you want to install A2A Client. Select **Next**. Do not use the space character in the name of any A2A Client installation folder, the root folder, or the installation subfolder.
6. In the **Server Information** window, enter the Fully Qualified Domain Name (FQDN) of the appliance in the **Server Name** field. select **Next**.
7. In the **Choose Log Directory** window, enter a path name for the installation log file directory or use the default path name. Select **Next**.
8. In the **Pre-Installation Summary** window, validate the installation information then select **Install**. The **Installing Password Authority Client** window appears and shows the progress of the installation. When the installation finishes, the **Install Complete** window appears.
9. Select **Done**.
10. If you are upgrading a pre-3.0.1 A2A Client and you want to use local storage caching, enable this caching. Only caching in memory is enabled by default.
  - a. Navigate to the A2A Client configuration file (`cspm_client_config.xml`). The file is in `cspm_client_home\cloakware\cspmclient\config`.
  - b. Set the `<preserveCacheBetweenRestarts>` tag to `true`.
  - c. From the Windows Services administrative tool, start the **cspmclientd** service.
  - d. Open a Command Prompt window and enter the following commands:
 

```
set CP=%CSPM_CLIENT_HOME%\cspmclient\lib\cspmclient.jar;%CSPM_CLIENT_HOME%\cspmclient\lib\bc-fips-1.0.0.jar

java -classpath %CP% com.cloakware.cspm.client.ClientDaemonManager authenticate
```
  - e. When prompted, enter a password for local authentication.

#### **WARNING**

Store this password securely. when the `<preserveCacheBetweenRestarts>` tag is set true, the password is required every time the A2A Client is started.

- f. Log in to the PAM UI.
- g. Navigate to **Credentials, Manage A2A, Clients**.
- h. Select the A2A Client and select **View** button.
- i. Select the **Change Key** button.

- j. Select **Close**.
11. Stop and restart the **cspmclientd** service:
  - If you use the Windows Services administrative tool, stop the **cspmclientd** service then restart it.
  - If you use a command window, enter: `net stop cspmclientd` followed by `net start cspmclientd`

### **Activate the Request Server on Windows**

After you install the A2A Client, [activate the request server](#).

## **Upgrade PAM SC Utility Appliances to Support PAM 4.1.x**

If you are using integrated PAM SC, deploy `pam-utility-appliance-1.0.0.09` patch to upgrade all active Utility Appliances (that is, members of Utility Groups) to support PAM.

### **Follow these steps:**

1. Download the `pam-utility-appliance-1.0.0.09.p.zip` patch archive from the [Broadcom Support](#) and extract its contents (a `.bin` and a `.sha256` file) to a local drive.
 

**IMPORTANT**

Do not discard downloaded patch files. If you later add Utility Appliances to a new or existing Utility Group, these patch files are required to reupload and restage each patch (unless you must change the existing Patch Level).
2. Open the PAM UI and navigate to **Configuration, Utility, Patches, Utility Appliance Patches**.
3. On the **Available Patches** tab, select **Upload**.
4. On the dialog that opens, select **Choose File**, locate, and select (`pam-utility-appliance-1.0.0.09.p.bin`), and then select **Upload**.
5. Verify that the file information is correct and select **Save**.
 

The patch is uploaded to the PAM server and the service updates that it contains are added to the list of patches that are available to stage.
6. Do the following steps for each listed Utility Appliance service patch.
  - a. Select the service patch and select **Stage**.
  - b. On the dialog that opens, verify that the patch information is correct and select **Yes**.

### **NOTE**

Take a note of the name of each patch that you stage to identify which services to update in Step 7.

7. Select the **Patch Level** tab and do the following steps to update each service that you staged in Step 6:
  - a. Select the appropriate entry from the following list of displayed services and then select **Update**.
    - `pam-dh`
    - `pam-loginintegration`
    - `pam-activemq`
    - `pam-config`
    - `pam-eventforwarder`
    - `reloader`
    - `pam-a2a`
    - `activemq-config`
    - `pam-policyorchestrator`
  - b. On the dialog that opens, select the new patch version from the drop-down box and select **OK**.

### **NOTE**

If no patch is staged for this service, the drop-down box is empty, and you cannot continue.  
The service is updated and the new patch version is displayed in the patch level list.

**NOTE**

For information about how to delete unused patches and view information about applied patches, see [Deploy and Manage Utility Appliance Update Patches](#).

# Introduction

Privileged Access Manager is an automated solution for privileged access management. Privileged Access Manager enables centralized management of local and remote high-risk users in physical, virtual, and cloud environments. The core product enables you to secure access to critical infrastructure for privileged and third-party users by combining device access control and privileged credential management:

- **Network-based Device Access Control:** Uses your existing identity and access management infrastructure to facilitate stronger or multi-factor authentication for privileged users. For more information, see [Access Control Overview](#).
- **Password Access Control (Credential Manager):** Provides password access control that enables you to manage the setting of, storage of, and access to passwords. For more information, see [Credential Manager Overview](#).

## Core Product Overview

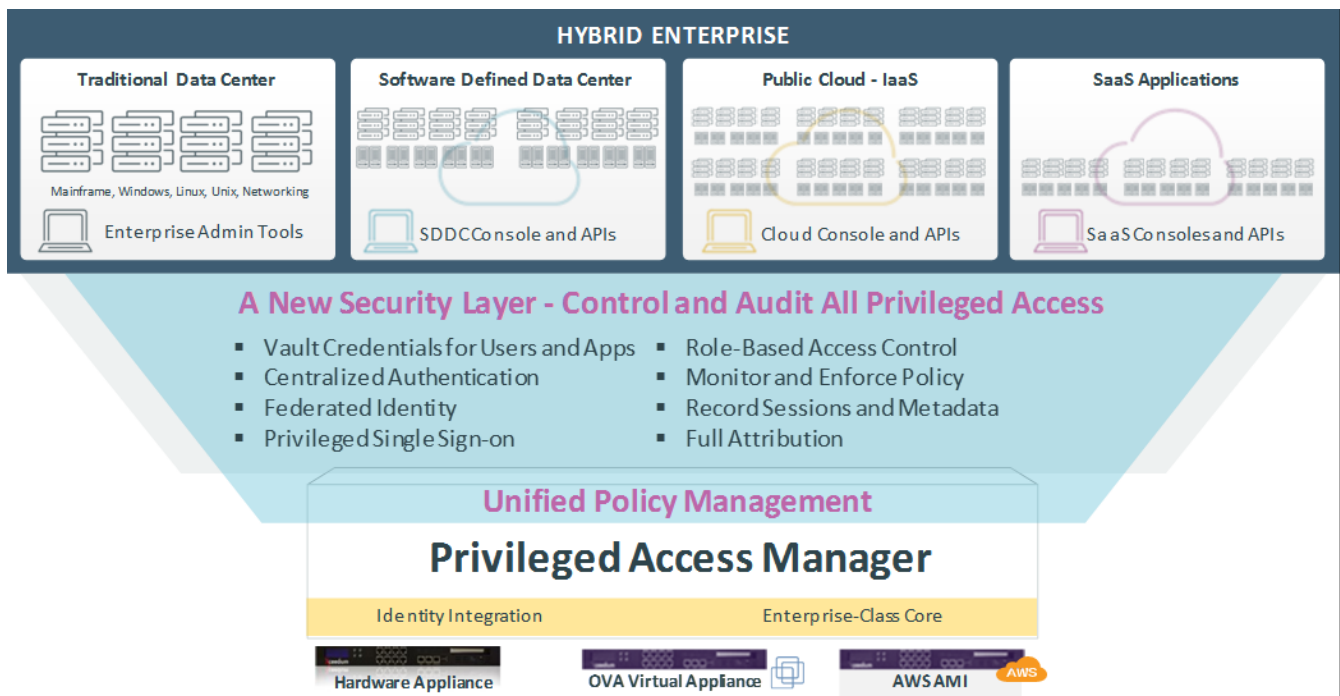
Privileged Access Manager core functionality enhances security by automatically doing the following tasks using policies that you define:

- Protecting sensitive administrative credentials such as root and administrator passwords
- Controlling privileged user access
- Monitoring and recording privileged user activity across all IT resources

PAM is available in the following form factors:

- Rack-mounted, hardened hardware appliance
- Open Virtual Appliance (OVA)
- Amazon Machine Instance (AMI)
- Virtual Hard Disk (VHD) for Azure

The following diagram provides an overview of the Privileged Access Manager solution.





These capabilities enable single sign-on by hiding credentials from the user while providing access to resources. Privileged users do not need to know anything about the target account. Privileged users only need their Privileged Access Manager account credentials. With Microsoft Terminal Services, user access can be further restricted to single Windows applications.

The product compartmentalizes high-risk users, alerting, remediating, tracking, recording, and reporting on all user activities inside the entire heterogeneous IT infrastructure. Administrators, application developers, vendors, and technical contractors can securely access critical IT resources from inside and outside the organization without gaining a footprint on the network. Auditors can monitor all user events and view centralized reports for accountability and testing of controls. You can use the product to balance audit and compliance requirements with the need for operational efficiency.

## **Core Functional Highlights**

Privileged Access Manager offers the following core features:

- **Granular Policy Enforcement**  
Policy enforcement compartmentalizes high-risk users using integrated Java applets with a reverse port-tunneling access technology that provides segregation of critical IT infrastructure components and separation of duties that easily meets compliance requirements. Users are contained within these compartments through the Symantec LeapFrog Prevention™ technology, which employs a whitelist/blacklist approach, blocking users from leaving authorized areas at the socket level.
- **User Activity Monitoring**  
User activity monitoring watches user activity with real-time alerts for attempted policy violations. Administrators are notified immediately when an access violation has been attempted, detected, and prevented. Access might be terminated when a user attempts to access an unauthorized system or device.
- **User Event Recording**  
User event recording provides centralized tracking of all activities and events using session recording and playback capabilities. An administrator can have complete visibility into user activities in CLI sessions. You can configure event recording that is based on individual user profiles or individual back-end devices. All command-line activity is monitored, recorded, and archived for audit and compliance purposes.
- **Centralized Reporting**  
Centralized reporting provides comprehensive, customized audit and compliance reports for any user-initiated events. The reports can include usage data and attempted security violations. You can also run automated reports that are focused on the compliance of individual users. You can configure the automated reports to run at predetermined intervals and then distribute the reports using email.

## **Other Capabilities**

Privileged Access Manager also offers the following other capabilities:

- **Secrets Management:** Provides access control for human users and programs to sensitive and privileged information (secrets). That information might include X509 certificates, connection strings, tokens, configuration parameters, encryption keys, credentials, and so on. For more information, see [Secrets Management Overview](#).
- **Host-Based Device Access Control (Unified PAM Server Control):** If enabled, *PAM Server Control* functionality adds the powerful *host-based security* capabilities from the standalone Privileged Identity Manager (PIM) and Privileged Access Manager Server Control (PAM SC) products. For more information, see [PAM Server Control \(Host-Based\) Access Control Overview](#).
- **Threat Analytics:** A powerful tool for identifying anomalies in PAM user behavior and implementing policies to dynamically mitigate potential insider threats or breaches by external threat actors. The Threat Analytics Console assists you in analyzing the collected data with rich graphical visualizations. For more information, see [Threat Analytics Overview](#).

## PAM (Network-Based) Access Control Overview

Privileged Access Manager network-based access control uses your existing identity and access management infrastructure. The appliance integrates with Active Directory and LDAP-compliant directories, and authentication systems like RADIUS. Integrated with advanced authentication tools like CA Advanced Authentication and others.

PAM access control facilitates stronger or multi-factor authentication for privileged users. In addition, the product fully supports enabling technologies like PKI/X.509 certificates and security tokens. Its support for Personal Identity Verification/Common Access Cards (PIV/CAC) ensures compliance with U.S. Federal Government HSPD-12 and OMB M-11-11 mandates.

PAM access control employs a unique "Deny All, Permit by Exception" (DAPE) security model to control access for high-risk users with zero footprint on the network. Users are granted visibility only to authorized areas. This security model also offers a centralized, secure access channel for administrators. Administrators gain a single point of entry and view to critical IT infrastructure.

The product also provides centralized tools for operational efficiency, and integration with centralized authentication policy engines.

**This section has the following other contents:**

### Access Target Devices

You can access a target device from Privileged Access Manager in one of these ways:

- Access Method – A proprietary Java applet to make a connection using one of several standard protocols (SSH, RDP, others)
- Service – Privileged Access Manager invokes a local third-party application from your client (for example, PuTTY on a Windows PC) to handle the connection
- RDP Application – Privileged Access Manager uses the RDP protocol to invoke a specific application on a target Windows OS Device

### Setting Up PAM access control

To set up PAM access control, create records that represent your managed objects. At the top level, your managed objects are the devices that you manage (and their properties) and user accounts.

The baseline-managed objects are devices and users. A policy is the relationship between a device (or device group) and a user (or user group). A policy specifies the tasks that each user is permitted to do with each device. A policy also can specify whether to record all or some of a user session with the device, permitted or not.

For more information, see [Configure Policies to Provision User Access to Devices and Applications](#).

## Credential Manager Overview

Credential Manager is a part of the Privileged Access Manager product. Credential Manager lets you manage how privileged credentials are set, stored, changed, and updated. Credentials include:

- Privileged account user name and passwords, such as UNIX `root`
- RSA key pairs
- Application-to-application (A2A) account credentials. A2A accounts are used by automated processes to access server resources. The A2A feature replaces credential instances that are embedded in insecure scripts and configuration files. These instances are replaced with a single instance in the secure appliance. You can then change server credentials as often as necessary and automate the management of server credentials.

This section introduces the following concepts:

## **Privileged Users**

Privileged accounts have the necessary rights to log and administer a system. The appliance recognizes and manages two types of privileged users:

- A person with rights to access and administer a system and the applications on that system. A privileged user likely uses shared, centrally stored credentials for access to a high-privilege target account. Examples of privileged accounts include the UNIX `root` account or a Windows Administrator account.
- A request script or application that automates a process. Such a script requires a centrally stored password to log in to an application using a privileged account.

Privileged users maintain accounts at the remote target system where the applications reside. These remote devices process or consume submitted credentials.

## **Credential Security**

Credential changes get recorded in a secure database on the appliance. Credential Manager encrypts target credentials before storing in a secure database. The cryptographic connector is the mechanism for storing credentials, and you can use this mechanism to customize how your credentials are encrypted. The cryptographic connector uses a 256-bit cryptographic kernel for maximum security.

## **Related Credential Manager Information**

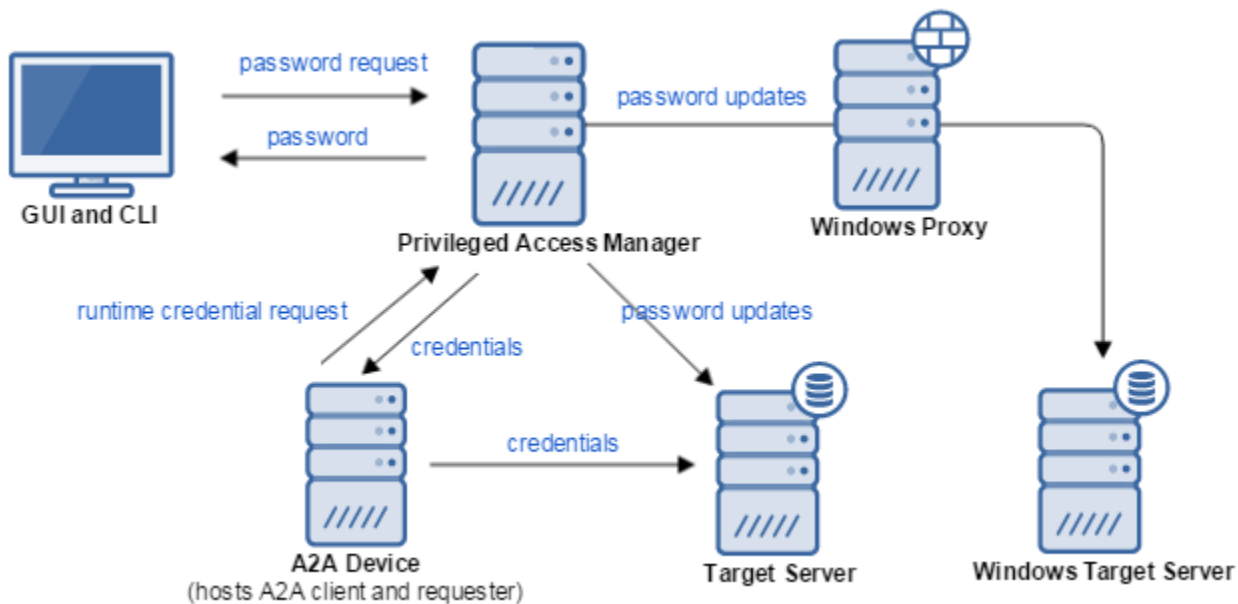
For more information about Credential Manager, use the table of contents to access the subtopics.

## **Credential Manager Components**

Credential Manager is integrated with the appliance. Credential Manager uses the following components:

- **UI and CLI:** You can configure Credential Manager features using the **Privileged Access Manager** UI or command-line interface (CLI).
- **Credential Manager Database:** The appliance is the centralized secure server and database that secures credentials.
- **Windows Proxy:** (Only required to support Windows target servers). The Windows Proxy is one of three Windows components available to manage passwords for Windows accounts. (The Windows Remote Connector and the Active Directory Connector are the others). The Windows Proxy also can manage Windows services and scheduled tasks. Unlike the other two Windows connectors, the Windows Proxy is installed on the remote server in your target domain.
- **A2A Client:** (Only available with the A2A license.) The A2A Client is software that runs on a request server. The A2A Client manages communication with the appliance and decrypts requested credentials.

The following graphic highlights some of the components:

**Figure 9: Credential Manager Components**

## Password Management and Requests

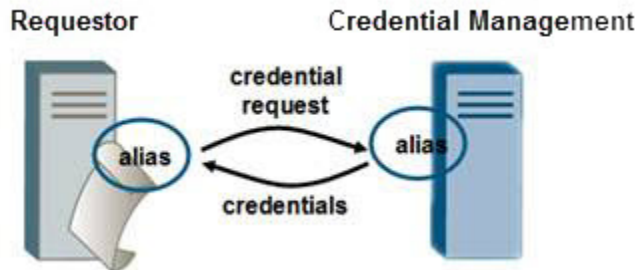
You can use the Credential Manager functions of PAM to manage passwords in the following ways:

- Change passwords on a regular schedule or when the password reaches a specified expiration. Scheduled password changes use automatically generated passwords that conform to your specified password composition policies. You configure password composition policies on a per target application basis.
- Configure password view policies and the actions that are taken after a password is viewed.
- Schedule password verification. If passwords become out-of-sync, Credential Manager can alert you.
- Allow authorized users to view current and historical target account credentials

### A2A Password Requests

You can integrate applications that use a hard-coded user name and password with Credential Manager. The integration lets you replace the hard-coded credentials with a runtime credential request and target alias. As shown in the following figure, Credential Manager uses the target alias to determine which credentials are being requested. The application requesting the target account credentials is known as the requestor. The server hosting the requestor is known as the request server. The activity of integrating your requestor with Credential Manager is known as A2A integration.

For requestors to retrieve credentials successfully, you must authorize them. Requestor authorizations are known as authorization mappings.



## Password Security

Credential Manager encrypts target credentials before storing them. When a requestor requests credentials, the credentials remain encrypted as they are transferred over the network. The A2A Client, which you must install on the request server, decrypts the credentials before passing them along to the requestor. For more information about cryptography in this product, see [Configure Enhanced Encryption for Stored Credentials](#).

## Policies to Create and View Passwords

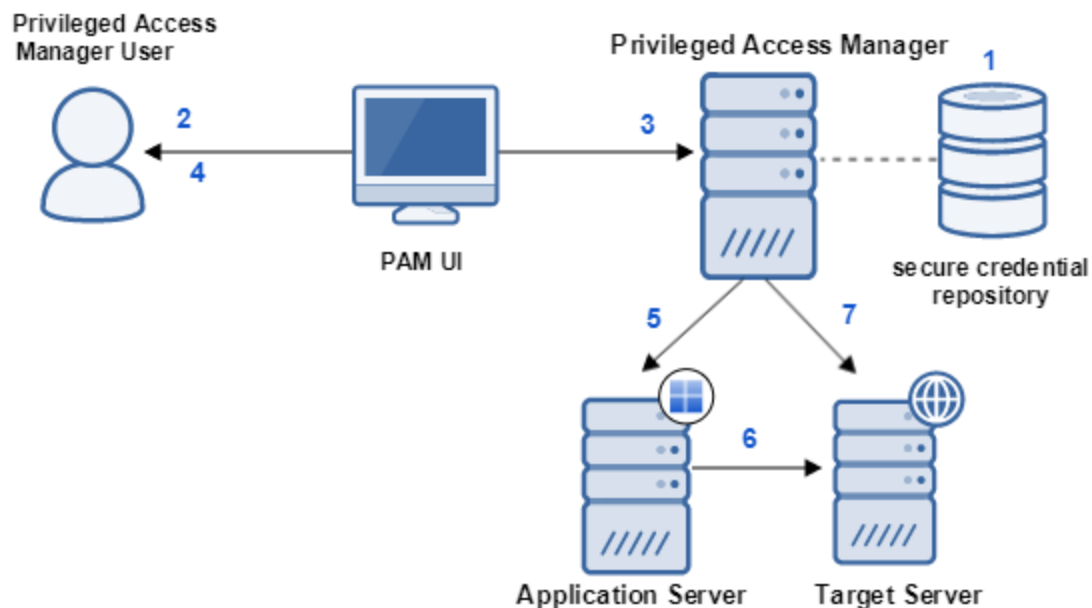
Credential Manager allows you to create policies to:

- Specify the rules to which passwords must conform to ensure that they meet the unique security needs of your organization
- Automatically change the account password for synchronized accounts once it is viewed
- Ensure that only one person at a time can view an account password
- Ensure that an account password is only revealed after a specific approver has authorized it

## How Does Password Management Work?

The following figure illustrates how Credential Manager provides password management for privileged users and A2A password requests.

**Figure 10: Password Management Flow**



**For privileged user password requests:**

1. Passwords are stored securely in a central repository on the appliance.
2. Administrators use the UI or CLI to authenticate themselves.
3. The administrator searches for the desired account or navigates to it.
4. If the password viewing policy allows, the administrator views the account password. If a policy specifies it, the password on the target can be updated automatically.

**For A2A password requests:**

5. An application requests a password from the appliance.
6. The application substitutes the credential into a connection string.
7. As determined by a password policy, the password gets updated on the target server and the appliance.

## Credential Manager Password Flow

Privileged Access Manager Credential Manager manages passwords for the following situations :

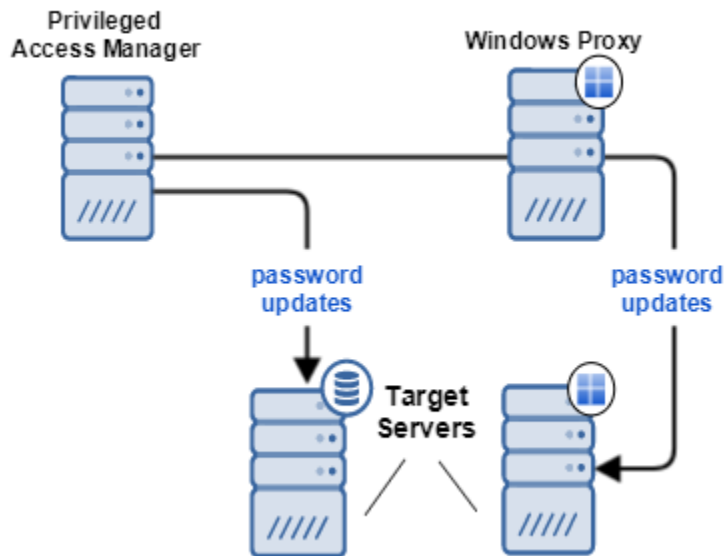
- Synchronized updates of target account passwords.
- A password request from an administrator to access a privileged account.
- A password request from an application to access a target account.

The following sections describe sample use cases.

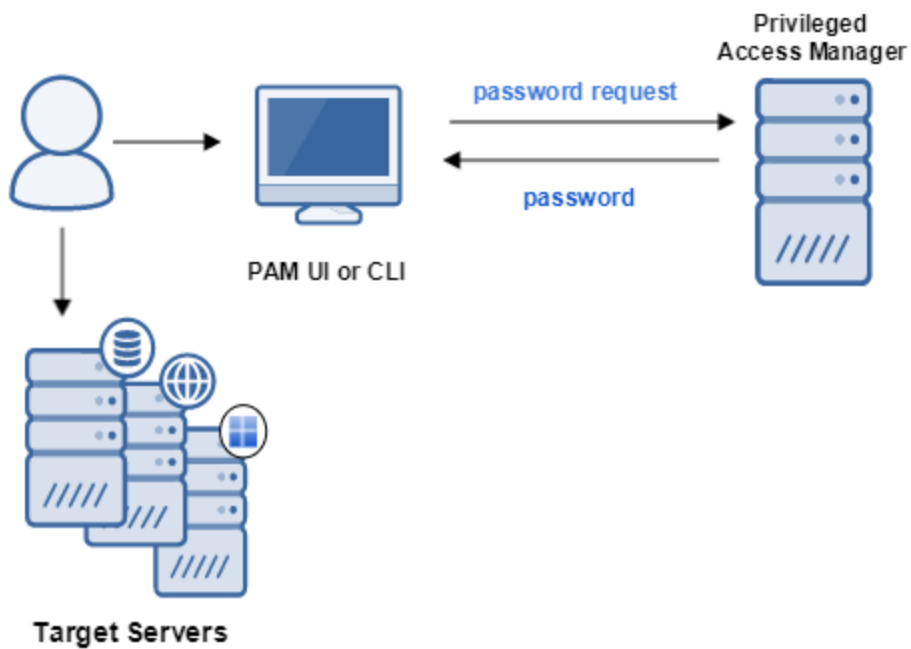
**Synchronized Target Password Updates**

When you add target account passwords in Credential Manager, it contacts the target server to validate that the password is correct. Once validated, target account passwords update directly in Credential Manager. This feature is named *target account synchronization*. The appliance initiates the flow for target account password updates and Credential Manager then pushes the new password to the target account.

When a target account is a Windows account or Windows service, the appliance directs the Windows Proxy to perform the password verification and update.

**Figure 11: Credential Manager Password Flow****Privileged Account Password Requests**

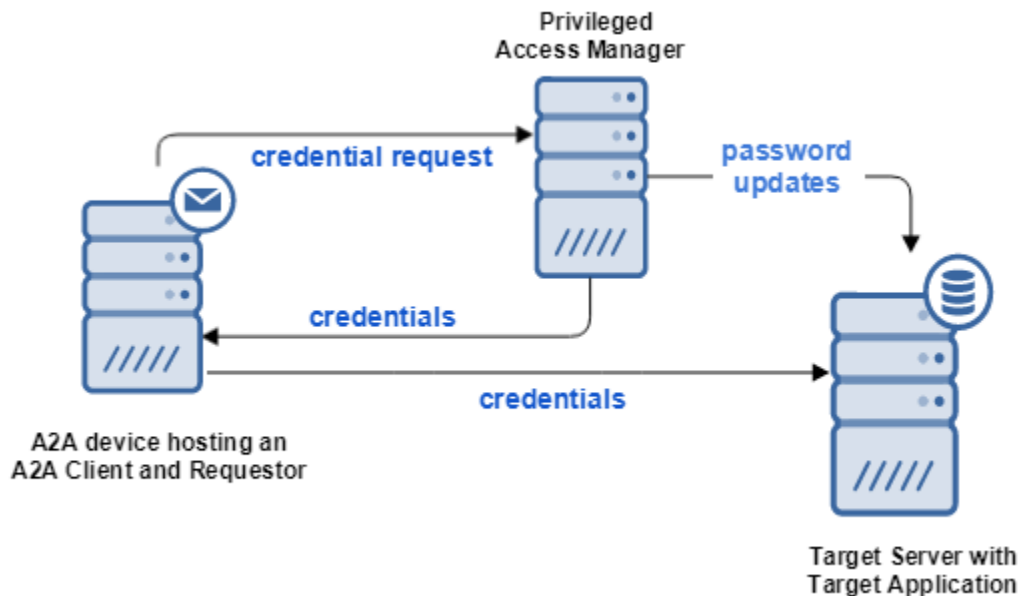
In this workflow, the user requires access to a privileged account. Using the GUI or CLI, the user requests the target account password.

**Figure 12: Privileged Account Access Flow**

## A2A Credential Requests

When an application requires target account credentials, the application sends the credential request at runtime to the appliance. The credential request includes the target alias that is associated with the account. If the requestor is authorized to access the target credentials, the appliance returns the credentials to the requestor. The requestor uses the account credentials to connect to the target application.

**Figure 13: A2A Credential Request Flow**



## Application-to-Application (A2A) Credential Management

Application-to-Application (A2A) credential management lets customer applications and scripts securely obtain credentials for target applications. A2A eliminates the need for customer applications and scripts to store credentials. The requesting applications and scripts are called *requestors*. The credentials are always encrypted and access is controlled and configurable. Also, the target account credentials can be changed at any time.

Review the following information to learn about A2A credential management:

### Benefits of A2A

A2A credential management offers the following advantages:

- Stores encrypted credentials. Credentials are not stored in plain text.
- Prevents unauthorized users from gaining access to credentials. An unauthorized user can access script source code or a configuration file containing the credential.
- A2A can determine whether unauthorized access occurs.

A requestor must obtain the credentials for a target application from PAM. To reduce the network traffic from the requester to the appliance, A2A provides a local secure cache on the request server. Based on configured password policies, PAM dynamically changes the credentials of a target account. These changes are pushed to the request servers to keep the local cache up-to-date. If credentials cannot be dynamically updated, the organization typically uses a fixed password or key on the target. The passwords or key are then hard-coded in the requestors. In such cases, there is significant overhead in coordinating changes to credentials simultaneously on the target application and all the related configuration

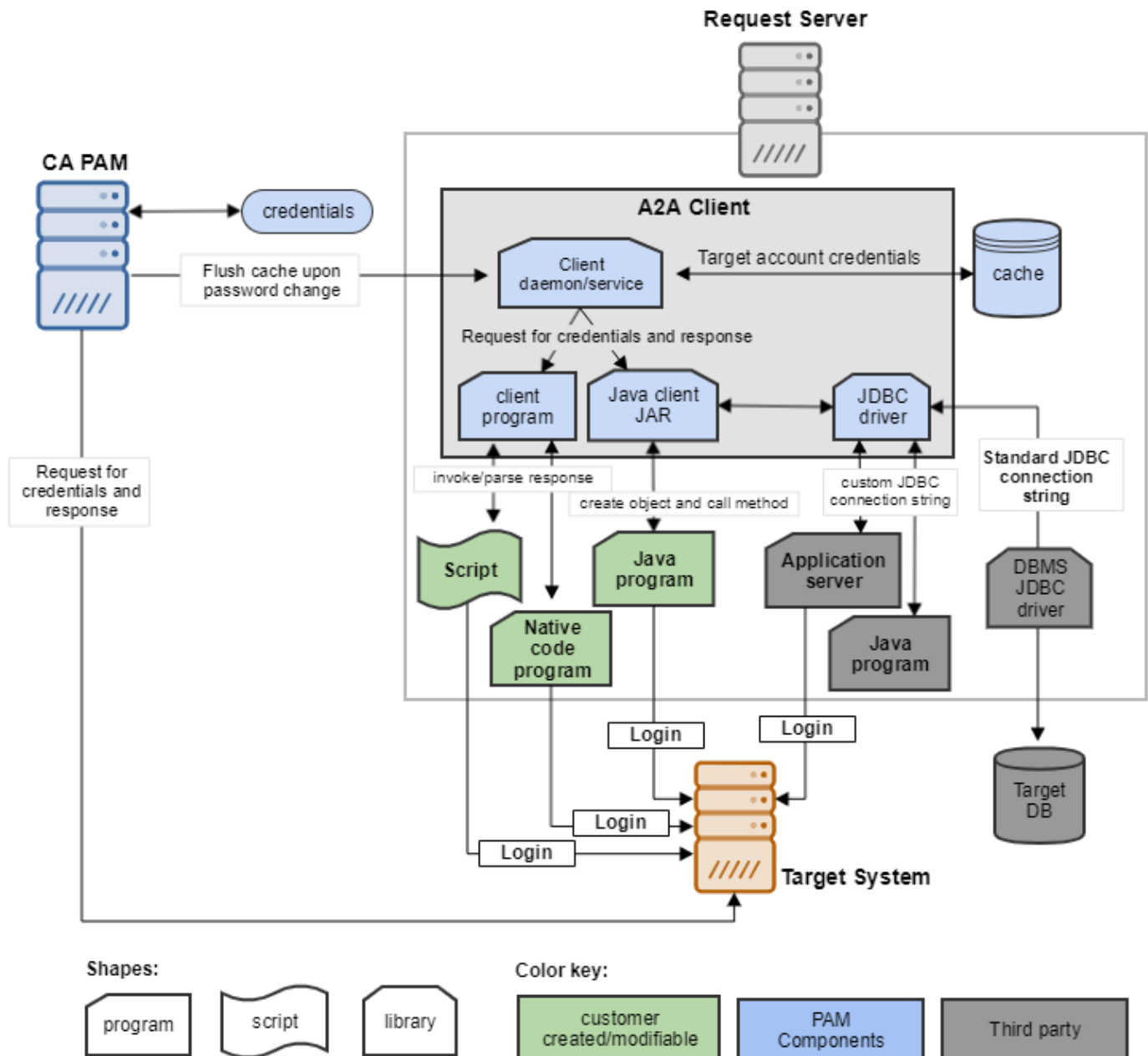


files and hard-coded scripts. The result is that credentials are not changed, which increases the potential for a data breach.

### A2A Components

The following diagram shows the components that are used to provide A2A credential management and how they interact.

**Figure 14: A2A Components**



The components are:

- **Requestor:** An application or a script that wants credentials to log in to a target application. For example, an OS, DBMS, or a customer-specific application.
- **A2A Client** which consists of a Client Program, a Java client JAR, a A2A JDBC driver, a Client Daemon or service, and runtime Cache:
  - The **Client Program** is an executable that is invoked from customer scripts and native code.
  - The **Java client JAR** interacts with a customer Java program. The Java client JAR contains a class with a method that is invoked to retrieve a password.
  - The **A2A JDBC driver** is a proxy JDBC driver that Java applications can use. A special connection string specifies the desired target alias and information for the DBMS-specific JDBC driver. The A2A JDBC driver forwards information to the DBMS-specific JDBC driver with the DB user ID and password that is obtained from Credential Manager.
  - The **Client daemon** (UNIX) or service (Windows) listens for requests from requesting applications or scripts. When a request arrives, the Client retrieves passwords. The Client also listens to the appliance for requests to flush the cache of account information when the account password is changed.
  - The **Runtime Cache** is a cache of account passwords and access information that is stored by the client daemon/service. This cache is stored locally to improve performance. The appliance notifies it when a password that it might contain has changed so that it can be removed from the cache.

The A2A Client is responsible for obtaining information about the program that invoked it, such as the program name, path, user executing the program, and hash.

- (Request) **Script:** A customer supplied script, in Perl, PHP, Python, UNIX shell (for example, sh, ksh, csh) that needs credentials for an account.
- **Native code program** or a **Java program:** An application that wants the credential for an account.

The following concepts also apply:

- Request Scripts are configured in the appliance by specifying the following information:
  - program request server
  - name
  - invocation path or the path on the file system and descriptors.

A registered Request Script specifies a Type. This field is optional.

- Request Scripts can be grouped to form a Requestor Group.
- A Target Account can be a Generic account an application-specific type such as UNIX, Oracle, Microsoft SQL Server. PAM cannot change the target password for Generic accounts but can change the target passwords of application-specific accounts. There might be multiple accounts with the same account name. The accounts might be on different servers or on the same server but with different target applications. PAM can effectively change the target password in these circumstances.

#### NOTE

For comprehensive information about the A2A feature, see [Manage Credentials Between Applications \(A2A\)](#).

## Secrets Management Overview

Use this section to understand Secrets Management in PAM.

Secrets management is access control for human users and programs to sensitive and privileged information. That information might include X509 certificates, connection strings, tokens, configuration parameters, encryption keys, credentials, and so on.

#### NOTE

Typically, credentials are used to authenticate an originating entity (such as a user or program) to a destination entity (such as a device or app). Credentials are a subset of secrets. However, credential management is handled separately. See [Credential Manager Overview](#) for more information on credentials.

PAM Secrets Management lets you control access to any information that your organization regards as secret, wants to protect, and wants to provide fine grained, auditable authorization. PAM gives Security Teams the ability to store, audit, and securely share this information with authorized recipients: people or processes.

PAM stores this information, or *secrets*, in a secure, encrypted vault.

PAM Secrets management provides the following general capabilities, among others:

- Administration
  - User Roles Management (granular roles for vault and secret management and access)
  - Vault Management (create, delete, update)
  - Secrets Management (create, delete, update)
- Access
- Process based, programmatic Authorization Mapping for Secrets (using A2A implementation)
- User-based Authorization Policies for Secrets (using the PAM UI/API)

See [Implementing Secrets Management](#) for instructions on configuring and using Secrets Management.

## PAM Server Control (Host-Based) Access Control Overview

This content introduces the functionality that is provided by the unified PAM Server Control Module and Utility Appliances.

By default, PAM provides network-based security by enabling centralized management of local and remote high-risk users over traditional physical hardware, virtual, and cloud environments. If enabled, *PAM Server Control* functionality adds the powerful *host-based security* capabilities previously provided by Privileged Identity Manager (PIM) and Privileged Access Manager Server Control (PAM SC).

Unified PAM SC provides host-based security for your most sensitive systems whether they are physical, virtual, or cloud-based. They provide active, comprehensive security software solution for open systems, tied dynamically to the operating system. Each time a user requests a security-sensitive operation, such as opening a file, substituting a user ID, or obtaining a network service, the product intercepts the event in real time and evaluates the validity of the operation before passing control to the native OS functions. Unifying this functionality with PAM adds powerful, fine-grained protection of operating system-level access and privileged user actions to its existing network-based security functionality.

For more information, see [Implementing PAM SC](#).

## Threat Analytics Overview

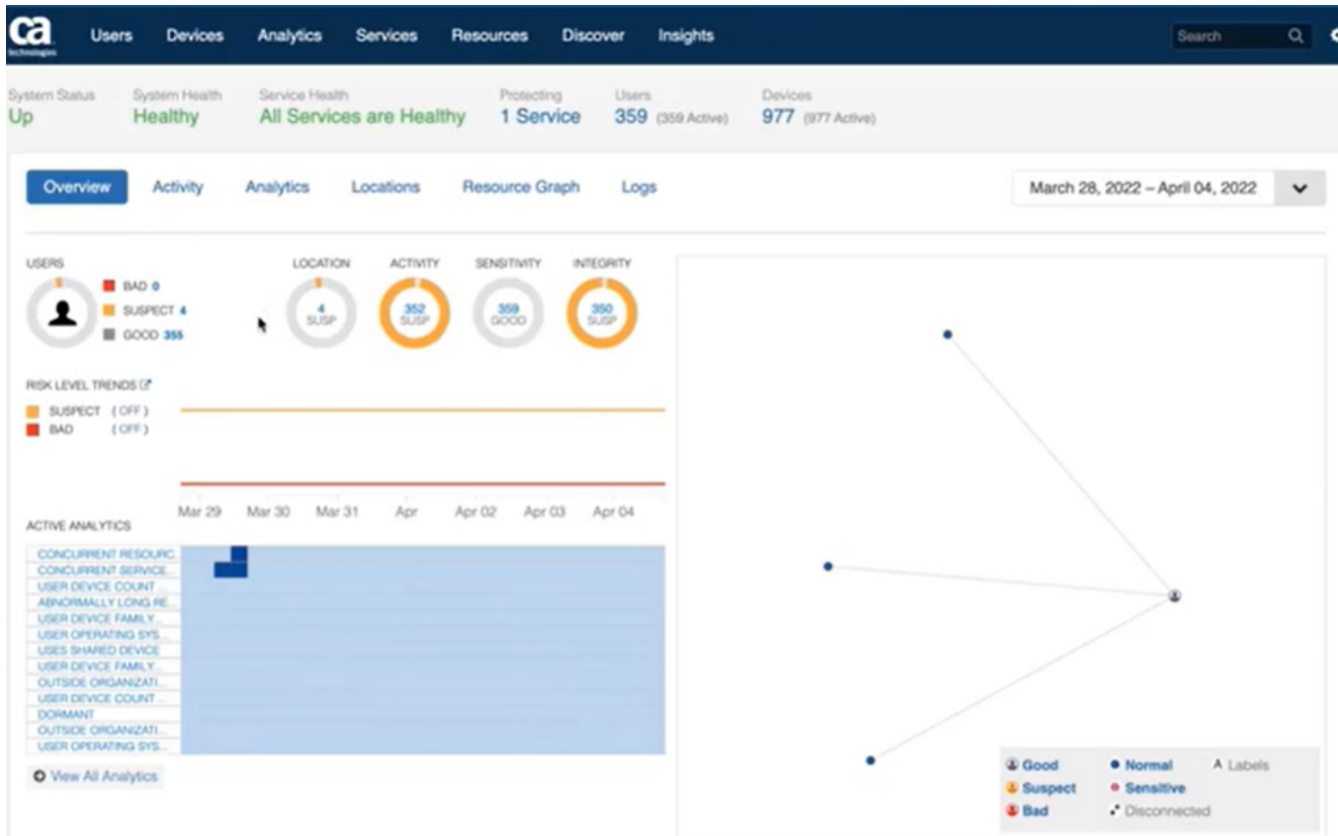
Threat Analytics is a powerful tool for identifying anomalies in PAM user behavior and implementing policies to dynamically mitigate potential insider threats or breaches by external threat actors.

Threat Analytics enables you to perform the following tasks:

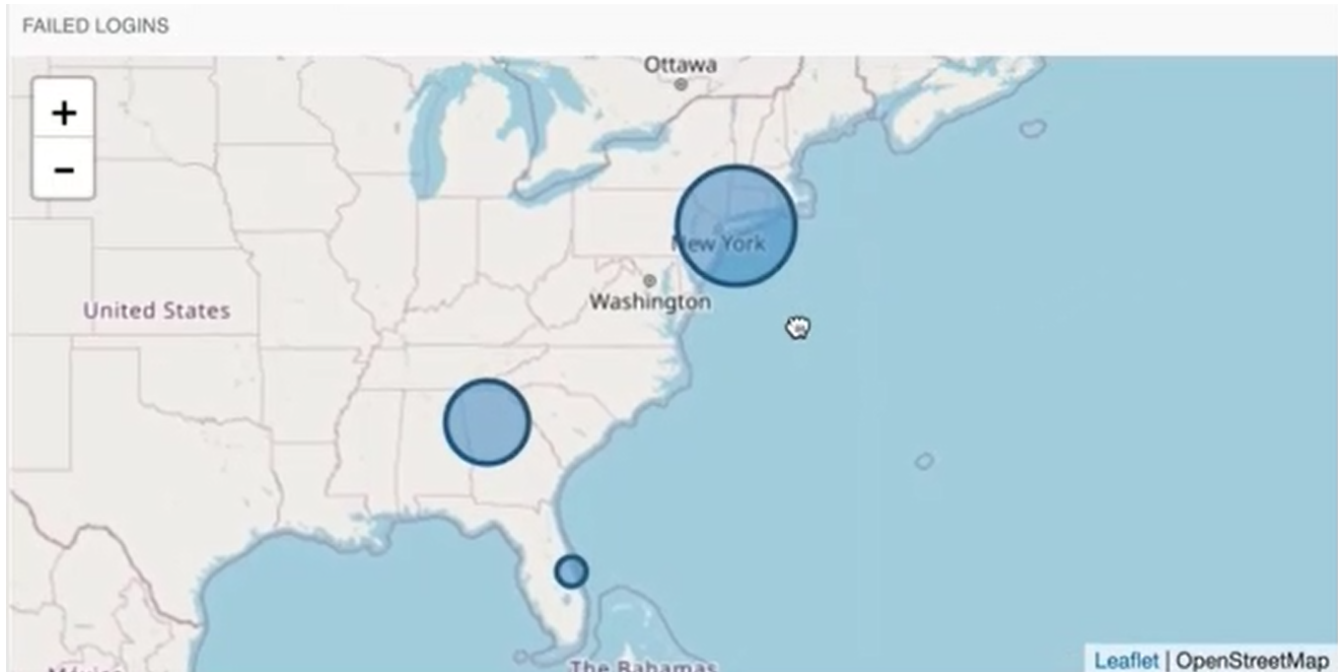
- Gather information on the threat landscape over time, from past events to the current moment.
- Configure policies and thresholds to dynamically mitigate against potential insider threats or breaches by external threat actors by triggering threat assessments for users or devices.
- Interpret, summarize, and filter network activity.
- Identify the threat landscape across an entire organization, from the overall threat snapshot down to the threat assessment for an individual user or device.

You interact with Threat Analytics using the *Threat Analytics Console*. The console provides graphs, maps, and other rich visualizations to help you analyze the threat data, as shown in the following examples:

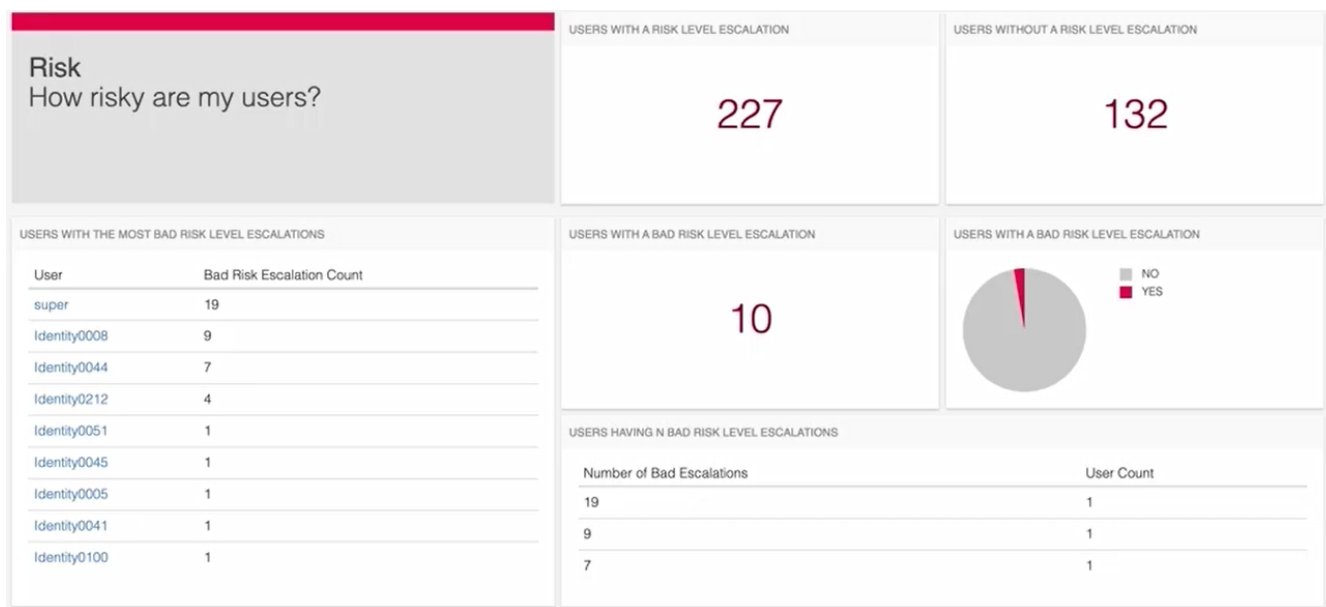
- View user and network threat activity at a glance:



- Use a geolocation view of the PAM network to see clusters of suspect users.



- Risk view shows counts of users with and without new risk level escalations and the number of users with Bad and Suspect risk-level escalations.



For detailed information, see [Implementing Threat Analytics](#).

# Deploying

---

You can deploy PAM as a hardware or software appliance. Learn how to deploy the product in different environments and how to set up clustering for high-availability deployments.

## Deploy Privileged Access Manager

The installation or deployment process varies according to which platform you use. The available options include:

- VMware OVA template
- Hardware appliance
- AWS AMI-based instance
- Microsoft Azure VHD

Members of a cluster must follow these rules:

- VMware OVA VM instances and the hardware appliance can be in the same cluster site. The AWS AMI instance can only be clustered with other AWS AMI instances in a cluster site. Similarly, a Microsoft Azure VHD instance can only be clustered with other Microsoft Azure VHD instances in a cluster site. Different sites in a multi-site cluster can run on different platforms.
- All cluster members must be running the same product release version. You can deploy the product in various ways to suit your existing security infrastructure.

## Product Deployment Infrastructure

- **Behind a Firewall**

Deploy the product in the DMZ directly behind a firewall to send high-risk users directly to Privileged Access Manager. This deployment protects devices against users that are authorized to perform upgrades, maintenance, development, and other administration activities.

**TIP**

For extra security in the DMZ, you can integrate the product with a RADIUS-based multifactor authentication solution like CA Advanced Authentication.

- **Behind an Existing VPN**

Deployment behind an existing VPN provides an extra level of control for high-risk users that are accessing resources through a standard VPN. In this scenario, Privileged Access Manager is connected to the existing internal network using independent, non-routed, non-bridged Gigabit network connections.

High-risk users who access the network through the standard VPN are routed to Privileged Access Manager for secondary authorization and device access. While the VPN keeps out unauthorized users, Privileged Access Manager keeps authorized users contained to only the devices they must access.

**NOTE**

SSL/VPN, which was supported in 2.x, is no longer supported in 3.x releases.

- **Parallel to an Existing VPN**

Deploy Privileged Access Manager in parallel to an existing VPN. High-risk users log in using an SSL connection. Privileged Access Manager authenticates these users and gives access to specific devices per a configured policy.

- **Between Virtual or Physical Networks**

Deploy the Privileged Access Manager between networks. The product provides access control and auditing of high-risk users that are granted access to a secure network segment. Access restricts users to only those devices and services necessary to perform their job.

- **In a Citrix XenApp Environment**

In a Citrix XenApp environment, Privileged Access Manager provides a complete entitlement management security framework. This framework enables companies to satisfy compliance and best practices for increasing numbers of high-risk users accessing the critical information technology infrastructure.

## IP Addresses and Ports for Network Connectivity

The ports that are listed in this topic are the default ports that Privileged Access Manager uses to establish network connectivity to target devices and managed services.

### Assign IP Addresses for the Appliance

Before you configure your network, assign and allocate IP addresses for the appliance. The hardware appliance has eight ports and the VMware OVA has 6.

### Review Port Assignments

The following table lists port assignment requirements for Privileged Access Manager or client workstations. Most connections use the TCP protocol, except for SNMP, NTP, and Syslog, which use UDP.

For AWS or Azure, ensure that the assigned ports are also open in the AWS or Azure network settings, and the OS instance firewall. Also, verify that the [AWS or Azure endpoints are open in the OS firewall](#).

For Credential Manager and the target connectors, you might have to open other ports. The target connector type determines the required port. For a detailed list of Credential Manager port requirements, see [Default Ports for Credential Manager](#)

#### NOTE

In the **Source** column, the term **Appliance** represents the Privileged Access Manager virtual or hardware appliance.

Port	Source	Destination	Notes
22	Appliance	SSH device targets	Required for target device access through a built-in SSH access method.
22	Administrator workstation	Appliance	Required for Remote PAM Debugging Services. This port is only available when the SSH Debug patch is installed and remote debugging is enabled.
23	Appliance	Telnet device targets	Required for target device access through built-in Telnet, TN3270, TN5250, or TN3270SSL access methods.
49	Appliance	TACACS server	Required for integration with a TACACS server.
123	Appliance	NTP servers	Optional for a standalone server, which is required for cluster nodes
135	Appliance	Windows target device	Required for Windows Remote connector use of WMI.

389	Appliance	LDAP server	Required for integration with an LDAP server
443	Client workstations	Appliance	Required for HTTPS access to Appliance.
443	PAM Client	Appliance	Users without installed Java can use the client instead of a browser.
443	PAM Access Agent	Appliance	Required for HTTPS access to Appliance.
443	Socket Filter Agent (SFA) on a target device	Appliance	Required for socket filter agent (SFA) use.
443	Appliance: cluster member	Appliance: cluster member	Required bi-directional communication between members of a cluster.
443	A2A Client	Appliance	Required for A2A Client use.
443	Windows Proxy	Appliance	Required for Windows Proxy use.
443	Management Console	Appliance	Required for the Management Console to open a client session with a managed cluster (VIP).
443	Primary Cluster Members	Management Console	Required for cluster to submit information to the Management Console.
443	SailPoint clientaz	Appliance	Use for SailPoint SCIM access to REST API.
445	Appliance	CIFS server	Required for integration with a CIFS server for session log storage.
445	Appliance	Windows target device	Required for Windows Proxy and Windows Remote connector use of SMB.
636	Appliance	Domain Controller	Required for Active Directory target application.
992	Appliance	TN5250 SSL targets	Required for target device access through a built-in TN5250 SSL access method.
1812	Appliance	RADIUS server	Required for integration with a RADIUS server.
2049	Appliance	NFS server	Required for integration with an NFS server for session log storage. The NFS server might also require port 111.
3306	Appliance	External MySQL log server	Required if external log server is configured.
3306	SailPoint	Appliance	SailPoint application uses STI to access PAM on this port.



3307	Appliance: cluster member	Other Appliance: cluster member	Required bi-directional between members of a cluster. This port is only open if the cluster is running, and only shows as open to port scans performed from another cluster member.
3389	Appliance	RDP target devices	Required for target device access through a built-in RDP access method.
5500	Appliance	RSA server	Required for integration with an RSA authentication server.
5900	Appliance	VNC target devices	Required for target device access using built-in VNC access methods.
5900	Appliance: cluster member	Other Appliance: cluster member	Required bi-directional between members of a cluster (Hazelcast). This port is only open if the cluster is running, and only shows as open to port scans performed from another cluster member.
8443	Appliance: cluster member	Other Appliance: cluster member	Required for internal HTTPS communication between cluster members.
8550	Appliance	Socket Filter Agent (SFA) on a target device	Required for socket filter agent (SFA) use.
13307	Appliance: cluster member	Other Appliance: cluster member	Required bi-directional between members of a cluster. This port is only open if the cluster is running, and only shows as open to port scans performed from another cluster member.
27077	Appliance	Windows Proxy	Required for Windows Proxy use.
28888	Appliance	A2A client	Required for A2A Client use.
TBD	Client workstations	Target devices	Any port to access configured services on target devices. The target devices are devices to which a PAM user is connecting using a local third-party application from the client.

### **Endpoint Addresses for AWS**

For AWS deployments, verify that the following endpoint addresses are also open in the OS instance firewall:

- **Commercial cloud:** iam.amazonaws.com
- **GovCloud:** iam.us-gov.amazonaws.com
- **AWS Policy:** sts.amazonaws.com

## Endpoint Addresses for Azure

For Azure deployments, verify that the following endpoint addresses are also open in the OS instance firewall:

- **Public Cloud:**
  - \*.azure.com
  - \*.microsoft.com
  - \*.microsoftonline.com
  - \*.core.windows.net
  - \*.graph.windows.net
  - \*.login.windows.net
- **US Government Cloud:**
  - \*.microsoft.us
  - \*.microsoftonline.us
  - \*.usgovcloudapi.net
- **China Government Cloud:**
  - \*.chinacloudapi.cn
- **German Cloud:**
  - \*.microsoftazure.de
  - \*.microsoftonline.de

## Download PAM Installation Media

This topic describes how to obtain the required installation media for PAM service pack (X.x.x) and major (X.x) releases.

### Download the Software for a Service Pack (X.x.x) Release

The software for service pack releases on the [Privileged Access Manager Solutions & Patches](#) page on the Broadcom Support site.

#### Follow these steps:

1. Open the [Privileged Access Manager Solutions & Patches](#) page in a new browser session. If you are prompted to log in, use your Broadcom Support credentials.  
A table containing all available component patches for each PAM service pack version opens.
2. Locate the **X.x.x Patches** section for your release.

The following table shows an example of the components available for a particular service pack:

Component	Description
CAPAM_X.x.x.p.zip	PAM Server update patch
remoteCLI-X.x.x.zip	RemoteCLI installer
AIXA2A-version.zip	A2A Client for AIX installer
WindowsA2A-version.zip	A2A Client for Windows installer
UNIXA2A-version.zip	A2A Client for UNIX installer
LinuxA2A-version-1.x86_64.rpm	A2A Client for RHEL RPM package
UNIXSFA-X.x.x.zip	UNIX SFA installer
WindowsProxy-X.x.x.zip	Windows Proxy installer
WindowsSFA-X.x.x.zip	Windows SFA installer

Component	Description
pam-utility-appliance-X.x.x.p.zip	Server Control Utility Appliance installer
PAMTA-X.x.x.vhd.zip	Threat Analytics VHD for Azure
PAMTA-X.x.x.ova.zip	Threat Analytics OVA for VMware

3. Select the link for the component software that you require and download the zip file to your local system.

**NOTE**


If you are running a service pack release but cannot find an entry for the component you require, download the version that is associated with the prior major release. For example, If you are running 4.0.3, download the 4.0 version. To locate the 4.0 version, follow the steps in [Download the Software for a Major \(X.x\) Release](#) and select the appropriate version in Step 6.

4. If necessary, copy the downloaded file or files to the systems where they are required.
5. If the download file is compressed, extract it to a local drive.

### **Download the Software for a Major (X.x) Release**

Download the installation media for a major PAM release from the Product section of the Broadcom Support Portal.

**Follow these steps:**

1. Open the [Broadcom Support Portal](#) in a new browser session. If you are prompted to log in, use your Broadcom Support credentials.
2. Select **Cyber Security Software** from the product selector (  ) drop-down list that is displayed to the left of your account name in the header.
3. Select **My Downloads** in the left pane.  
The **My Downloads - Cyber Security Software** page opens, listing your licensed products.
4. Select **PRIVILEGED ACCESS MANAGEMENT** from the list.
5. Filter the results to locate the required components:
  - For most components, filter the results to locate one of the following product entries
    - **PAM DEBIAN X.x** or **PAM with FIPS DEBIAN X.x** (as required)
    - **PAM Virtual Appliance DEBIAN X.x** or **PAM Virtual Appliance with FIPS DEBIAN X.x** (as required)

The following table shows an example of the major release components that are listed after selecting any of the previous product entries:

Component	Description
Privileged Access Manager rX.x.ova	PAM Server OVA for a hardware or VMware appliance
Privileged Access Manager rX.x with FIPS.ova	PAM Server OVA with FIPS for a hardware or VMware appliance
Privileged Access Manager rX.x for Azure.tgz	PAM Server VHD for Microsoft Azure
Privileged Access Manager rX.x for Azure with FIPS.tgz	PAM Server VHD with FIPS for Microsoft Azure
Privileged Access Manager Upgrade Patch rX.x.zip	PAM Server upgrade patch (for all appliance types)
Privileged Access Manager Utility Appliance rX.x.ova	PAM Utility Appliance OVA
RemoteCLI rX.x.zip	RemoteCLI installer

Component	Description
Unix Socket Filter Agent rX.x.zip	Unix Socket Filter Agent installer
Windows Proxy rX.x.zip	Windows Proxy installer
Custom Connector Framework rX.x JDK 8.zip	Custom Connector Framework JDK 8 installer
Custom Connector Framework rX.x JDK 11.zip	Custom Connector Framework JDK 11 installer
Privileged Access Manager SC Migration Utility rX.x.iso	PAM SC Migration Utility ISO image
Privileged Access Manager SAM Data Extraction rX.x.iso	SAM Data Extraction Utility ISO image

- For Credential Manager A2A Clients, filter the results to locate the **PAM App to App Manager** or **PAM App to App Manager with FIPS DEBIAN** (as required) software. The following table shows the major release components that are listed after selecting either of the previous product entries:

Component	Description
Windows A2A Manager (Client) rX.x.zip	Credential Manager A2A Client for Windows
Unix A2A Manager (Client) rX.x.zip	Credential Manager A2A Client for UNIX
AIX A2A Manager (Client) rX.x.zip	Credential Manager A2A Client for AIX

6. Select the required software component.
7. Select the required version from the **Release** column.  
The **Primary Downloads** page opens, listing all the available product downloads for the selected version, as shown in the following example:

← **PAM DEBIAN 4.1** ? Product Download Help

Primary Downloads Search 4.1 DEBIAN 0000 English

[Download Selected](#) ☒ Expand All

---

PAM Virtual Appliance Release 4.1 Service Pack 0000 Packlist ID 511488 ⏏

File Name	Last Updated	SHA2	MD5	Download	Tokens
<b>Custom Connector Framework r4.1 JDK 11.zip</b> 62.45 MB	Apr 28, 0022 12.00AM	8439d8a4cc8563ca78c1f3631a68c becad1401649998c5a8594c0412d 6662fa7	18fe2b586645211fa7d849b179394 a2a	<input type="checkbox"/>	<a href="#">Generate</a>
<b>Custom Connector Framework r4.1 JDK 8.zip</b> 65.27 MB	Apr 28, 0022 12.00AM	cc2a78fc76052c09e8812a0c52c15 1a7d43c835bca3aee91c5c8191fe6 ff9f9e	1ad9d1631c746dead057f58267b0 5600	<input type="checkbox"/>	<a href="#">Generate</a>
<b>Privileged Access Manager SAM Data Extraction r4.1.iso</b> 197.23 MB	Apr 27, 0022 12.00AM	96748974508d88ce510fe754ef9dc 4871aa6c2fa0e8dfe92a6f593b044 057bd0	d275a1562736b02fed42f87e7601 6cbf	<input type="checkbox"/>	<a href="#">Generate</a>
<b>Privileged Access Manager SC Migration Utility r4.1.iso</b> 212.91 MB	Apr 27, 0022 12.00AM	ed2e47aadc18570bdfc2e59216d1 56ea1a5e51919886945a23ee2230 5ce32fcf	fd75a7c989e6130e34f80ecc87208 84c	<input type="checkbox"/>	<a href="#">Generate</a>
<b>Privileged Access Manager Upgrade Patch r4.1.zip</b> 2.49 GB	Apr 27, 0022 12.00AM	afb30c007d407909b907b26202f44 46eff683f7d9b62960d351b42f82fbf da1a	3f664d36b67f853a2d45af1931b98 c90	<input type="checkbox"/>	<a href="#">Generate</a>
<b>Privileged Access Manager Utility Appliance r4.1.ova</b> 2.41 GB	Apr 27, 0022 12.00AM	8d18e808b8c05adcc7303e2aab3a c93cefddeb8835b52510f7bb3258d5 a729ab2	486fcc78759343e826327081752c 523a	<input type="checkbox"/>	<a href="#">Generate</a>

8. Use the available controls to download your required component file or files.

#### NOTE

For more information about how to use the controls and generic information about this procedure, select the **Product Download Help** button in the top-right (which is highlighted in the previous screenshot).

9. If necessary, copy the downloaded file or files to the systems where they are required.  
10. If the download file is compressed, extract it to a local drive.

## Deploy the VMware OVA Template

You can deploy Privileged Access Manager as a virtual appliance using a VMware OVA template.

First, deploy the VMware OVA template then configure the virtual appliance network settings. Before you can configure the network settings, the Privileged Access Manager license is required. After you upload the license, configure the network connection so that it can autoprovision (import) your virtual machine devices.

## **Download the Virtual Appliance OVA Software**

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

## **Deploy the OVA Template**

Deploy the Virtual Appliance OVA within a VMware ESX or ESXi environment.

### **Follow these steps:**

1. Log in to the vSphere Virtual Infrastructure Client or vSphere web client.
2. Select **File, Deploy OVA Template**. In the web client, select **Home, VMs and Templates**. Right-click the vCenter, and select **Deploy OVF Template**.
3. Browse to the location of the OVA file and select the file and select Open.  
The OVA template is imported. Continue with the rest of the configuration. Select Next to move through the configuration.
4. In the Name and Location settings:
  - a. Enter a new name for this appliance.
  - b. In the **Inventory Location**, select the data center location where you want to install PAM. Select **Next**.
5. For the **Host/Cluster** settings, specify the host or cluster location where you want to deploy the template.
6. For the Storage, select where you want to store all data files that are associated with the VM.
7. For the Disk Format, select **Thick Provision Eager Zeroed**. Thin Provisioning is not supported.
8. Accept the remaining default settings.
9. Review the settings. Verify that the **Power on after deployment** check box is **not** selected.  
If any setting is changed, failure to keep this box unchecked results in redeployment of the OVA template. Edit the settings before the first power-up cycle of the guest VM instance.
10. Select Next.  
The OVA template is imported into the VMware host, cluster, or data center location that you previously selected.

The VMware virtual appliance deployment is complete. Go to the next section to edit the virtual machine settings.

## **Edit the Virtual Machine Settings**

The tasks that are required to set up the virtual machine settings include:

- Add network adapters
- Modify virtual RAM and CPU settings

### ***Add Network Adapters***

The OVA template ships with one virtual network adapter out of the box. The virtual appliance supports a total of eight virtual network adapters per virtual machine.

You can add the additional virtual network adapters even if there are no immediate plans to use them. Doing so allows for expansion when redeploying a new virtual appliance.

### **WARNING**

Add the virtual network adapters *before* the first power-on cycle of the virtual appliance.

### **Follow these guidelines:**

- Add virtual network adapters two through eight.
- If you are deploying adapters on ESX/ESXi hosts, select the right VM network.
- Select the correct network adapter type (Host Only, Bridged, or NAT) when adding virtual network adapters.
- Optional: If the deployment only requires one virtual network adapter, set adapters two through eight so they do *not* connect when the virtual appliance powers on.
- Optional: Set all virtual network adapters with static MAC addresses. You can set a static MAC address that contains the VMware OUI prefix in compliance with the following format:

00:50:56:XX:YY:ZZ XX is a valid hexadecimal number between 00 and 3F

YY and ZZ are valid hexadecimal numbers between 00 and FF.

Do not set the value for XX greater than 3F. Otherwise, the address might conflict with MAC addresses that the vSphere vCenter Server generates, or addresses that are assigned to the adapters for infrastructure traffic. See the VMware vSphere documentation for more information about VMware OUI allocation. To generate MAC addresses that meet the requirements, third-party sites are available.

### ***Adjust Virtual RAM and CPU Settings***

See the Virtual Instances section of the [Installation Requirements](#) page for guidance on configuring RAM, CPU, and storage.

### **Clone and Launch the Virtual Machine Instance**

After the virtual appliance settings are complete, complete the following steps:

1. Take a snapshot of the instance and make a full clone. This newly cloned instance serves as the new template for future deployments in your environment.  
Any changes to the virtual machine settings require a new full clone.
2. Launch a new virtual appliance instance from the cloned VM.
3. Power on the virtual machine.  
After the boot process is complete, the Virtual Utility Console displays in the VMware Virtual Console.
4. Configure the network settings using the Virtual Utility Console.

### **Configure Network Settings**

For initial network configuration, configure a default gateway and one or more network interfaces. These first steps enable the virtual appliance to connect to a network.

#### ***Basic Network Setting***

From the Virtual Utility Console, configure the settings for the first IP address. For other interfaces, you can use the Privileged Access Manager user interface.

The Main Menu of the console shows which keys are used to navigate through each menu.

#### **Follow these steps:**

1. From the Main Menu of the utility console, select **Basic Network Settings**. The Network Setup screen appears.
2. For the Default Gateway field, enter an IP address of the virtual appliance.
3. Specify a name as the host name for the virtual appliance.
4. Set the Domain (if applicable)
5. Save your configuration. You return to the Main Menu.

#### ***Interface Network Settings***

Enable the required network interfaces for the virtual appliance.

#### **Follow these steps:**

1. From the Main Menu, select **Interface Network Settings**.

2. For each network enabled network interface, enter an IP address. At least one interface is required.
3. Set the subnet mask for each enabled network interface.
4. Save the configuration.
5. From the Main Menu, restart Networking.
6. Verify that the network configuration is valid by contacting (pinging) the configured IP address from another PC.

The remaining configuration steps can be completed from the Privileged Access Manager user interface or Workstation Client.

## Deploy on an AWS Amazon Machine Image (AMI)

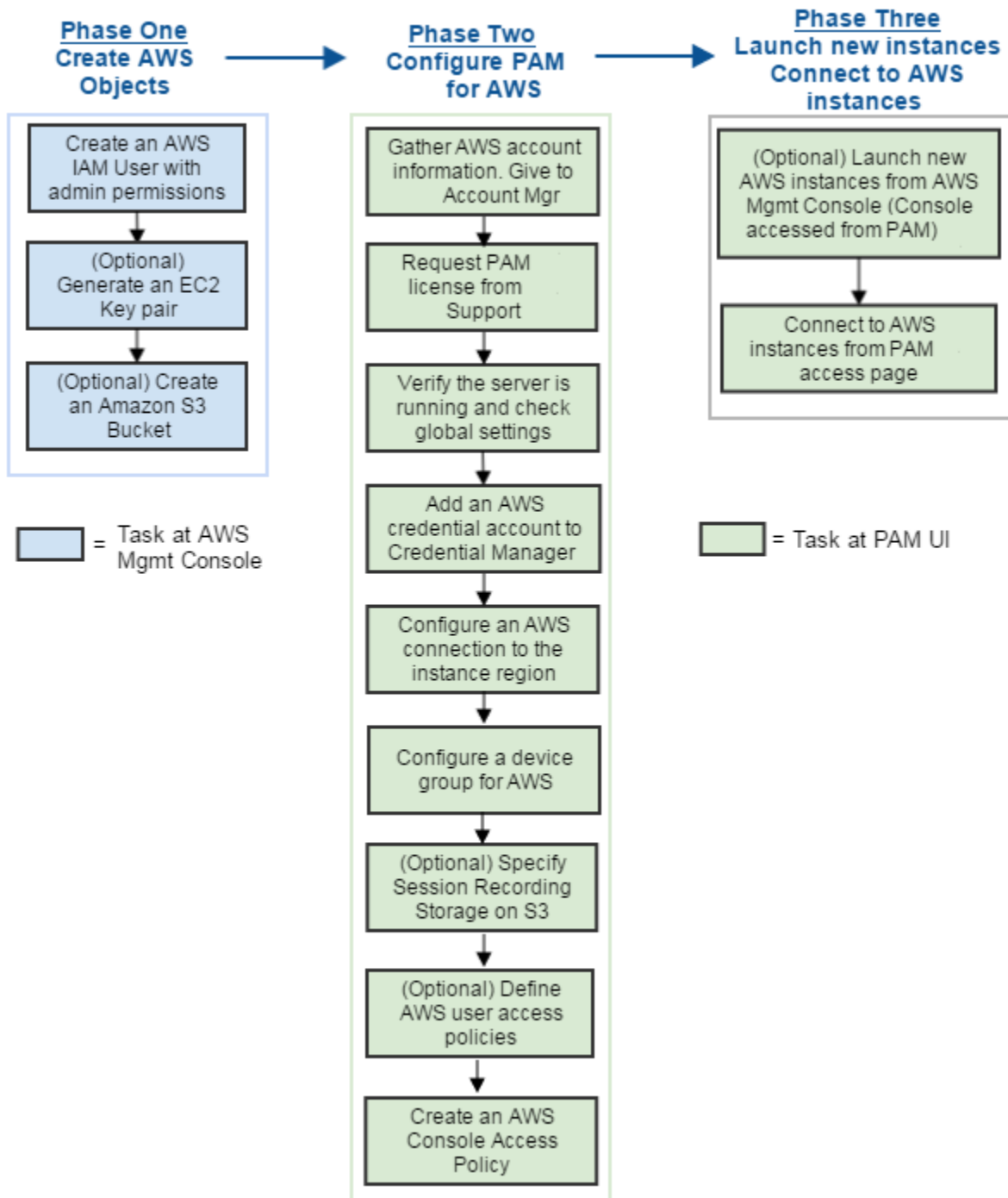
You can deploy PAM in the cloud on an AWS AMI virtual appliance. Privileged Access Manager can integrate with AWS in the following ways:

- Auto-discover AWS EC2 instances.
- Store access keys and use key pairs for auto-login.
- Use Amazon S3 buckets to store session recordings.
- Access the AWS Management Console through PAM, based on a policy.

The AMI acts as a template from which you can launch an instance.

Deployments tasks for an AWS AMI involve the following procedures:



**Figure 15: AWS AMI Deployment Task Flow**

The setup procedures are detailed in the following topics:

- [Create AWS Objects](#)
- [Configuring Privileged Access Manager for AWS](#)
- [Launch New Instances \(Optional\)](#)
- [Connect to AWS Instances](#)

## Create AWS Objects

Before you can integrate Privileged Access Manager with AWS, complete the AWS setup from the AWS Management Console.

These procedures explain how to create the following AWS objects:

- An IAM user with an Access Key ID and Secret Access Key pair. These procedures use the sample name **cademo-key-pair**.  
This key pair is assigned to the AWS instances that you can launch later.
- A uniquely named S3 bucket for storing PAM session recordings (optional).

Complete the following tasks at the AWS Management Console.

### Add an AWS IAM User with Administrator Permissions

Add an AWS IAM user with security credentials and permissions that allow integration between PAM and AWS.

1. Log in to the AWS Management Console.
2. Navigate to **IAM Dashboard, Users**, and select **Add User**.
3. Enter a user name. These procedures use **cademo** as an example.
4. For the Access type, select **Programmatic access**.  
If access to the Management Console is necessary, also select the **AWS Management Console Access** option.
5. Select **Next: Permissions**.

## Add user



Details



Permissions



Review



Complete

### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[+ Add another user](#)

### Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type\* ☒ **Programmatic access**  
 Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☐ **AWS Management Console access**  
 Enables a **password** that allows users to sign-in to the AWS Management Console.

\* Required

[Cancel](#)

[Next: Permissions](#)

6. In the Set Permissions screen, select **Create group**.
7. Select the **Show User Security Credentials** link.
8. Note the Access Key ID and the Secret Access Key values.
9. Select **Download Credentials** and download the **credentials.csv** file. Handle this file securely.
10. Select **Close** to return to the list of users.
11. From the list of users, select the entry for the cademo user to display the summary screen.
12. Select the **Permissions** tab then select **Attach Policy**.
13. Attach the following policies to the user. Use the search filter to narrow the list of policies.
  - **AdministratorAccess**. This policy permits federated access to the AWS Management Console.
  - **AmazonEC2ReadOnlyAccess**. This policy lets you import and discover AWS instances and import them into PAM.
  - **AmazonS3FullAccess** (optional). This policy is optional. Use the policy to read and write PAM session recordings to a mapped S3 bucket.
14. After selecting all relevant policies, select **Attach Policy** to return to the Summary page for the user. Review that all the permissions are set.

The following screen shows an example summary screen with only two policies:

Dashboard

Search IAM

Details

Groups

**Users**

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

IAM > Users > cademo

Summary

User ARN: arn:aws:iam::382034523008:user/cademo

Has Password: No

Groups (for this user): 0

Path: /

Creation Time: 2016-05-11 17:32 EDT

Groups Permissions Security Credentials Access Advisor

Managed Policies

The following managed policies are attached to this user. You can attach up to 10 managed policies.

[Attach Policy](#)

Policy Name	Actions
AmazonS3FullAccess	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>
AmazonEC2ReadOnlyAccess	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>

### Generate an EC2 Key Pair (Optional)

Generating an EC2 key pair depends on the following conditions:

- If there are existing key pairs for existing target instances in your AWS account, you do not need to generate a key pair. However, you must add all existing key pairs to the Credential Manager target account. PAM must have the key pair to access these instances and can manage the key pairs. Adding key pairs is done using the PAM UI.
- If you have a new AWS account with no instances, you must generate an EC2 key pair.

To authenticate to an AWS instance, obtain an EC2 key pair. When you launch an AWS instance later, you must provide this key pair.

1. In the AWS Console, navigate to **EC2 Dashboard, NETWORK & SECURITY, Key Pairs**.
2. In the navigation bar, select any region available to you regardless of your location. You cannot share key pairs between regions.
3. Select **Create Key Pair**.  
You are prompted to enter a key pair name.
4. Enter a name then select **Create**. For this procedure, the example name is **cademo-key-pair**.  
The key pair file, such as **cademo-key-pair.pem**, automatically downloads.
5. Store the key file in a safe location.

#### TIP

Amazon EC2 stores the public key only, and you store the private key. Securely storing the private key pair is important because the AWS Administrator role is associated with the pair. To manage the keys securely, see AWS documentation.

### **Create an Amazon S3 Bucket (Optional)**

If you want to keep session recordings on premise and not in AWS, skip this procedure. To store session recordings in an S3 bucket, create an Amazon S3 bucket.

To store session recordings in an Amazon S3 bucket, follow these steps:

1. From the AWS Management Console, open the Amazon S3 Console.
2. Select **Create Bucket**.
3. Specify a **Bucket Name** and select a **Region**.
4. Select **Create** to see the new, empty bucket.

For more information, see [Amazon S3 documentation](#).

#### **NOTE**

[Configure Privileged Access Manager for AWS](#)

## **Configure Privileged Access Manager for AWS**

Configure Privileged Access Manager for AWS by completing the following procedures:

### **Gather AWS Account Information**

Gather the following information and provide it to your Broadcom account representative:

- Your AWS account number
- The regions where you plan to deploy the instance.  
The following regions are supported:
  - US East (Ohio)
  - US East (Virginia)
  - US West (N. California)
  - US West (Oregon)
  - US GovCloud (East) - Only for US government customers
  - US GovCloud (West) - Only for US government customers
  - Canada (Central)
  - EU (Frankfurt)
  - EU (London)
  - EU (Paris)
  - EU Central-2 (Zurich)
  - EU-South-1 (Milan)
  - EU-South-2 (Spain)
  - EU West (Ireland)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - South America (Sao Paulo)
- Know the Privileged Access Manager version that you plan to use.
- Indicate whether you purchased the FIPS option.

Broadcom makes the appropriate AMI available to your account in the desired region, and sends you the AMI ID and Name.

### **Request a License from Broadcom Support**

A Privileged Access Manager license is required before you can connect with the AWS instance.

1. In the Privileged Access Manager UI, select **Configuration, Network**.  
The Network Configuration screen opens.
2. Open the **System Info** page and select **Hardware Identifiers**.
3. Copy the string in the **Hardware ID** field and provide it to the Broadcom licensing team to get a license.

### **Verify that the Appliance is Running and Check Global Settings**

Verify that the Privileged Access Manager appliance is running and that you can access it from the web UI or PAM Client.

This procedure assumes that the appliance is deployed in AWS, but that setup might not be the case. If Privileged Access Manager is deployed as a hardware appliance or as a VMware OVA, the appliance can still manage access for AWS instances.

#### **Follow these steps:**

1. From the UI, select **Settings, Global Settings**.
2. Confirm the values of the following settings.  
Basic Settings
  - **Login Timeout (Minutes):** 10
  - **Applet Timeout (Minutes):** 10
  - **Default Device Type:** Select **Access** and **Password Management**
 Warnings
  - **Show Recording Warning** is selected.
 These settings are not specific to AWS, but setting them globally is recommended.
3. Select **Save**.

### **Add AWS Account Credentials to Credential Manager**

To coordinate with AWS, store your AWS account credentials in a target account record in Credential Manager.

#### **Follow these steps:**

1. Log in to the UI and select **Credentials, Manage Targets, Accounts**.
2. Select **Add** to add an account.
3. In the **Application Name** field, select the magnifying glass and select **AWS Access Credential Accounts**.
4. Verify that the **AWS Credential Type** is set to **Access Key**.
5. Find and open the **credentials.csv** file that you downloaded.
6. From the values in the credentials.csv file, configure the following fields:
  - **Account Name**
  - **Access Key ID**
  - **Secret Access Key**
7. Select **Save**.  
The credentials are stored in PAM.
8. As a precaution, make a backup of the credential.csv file and securely store it off line. After securing the backup file, securely delete the credential.csv file from the users desktop.

### **Add an EC2 Private Key to Credential Manager (Linux Instances only)**

To auto-login to AWS Linux instances, add the EC2 private key file that you generated in AWS. By saving the key, you can log in to every AWS Linux instance that has **ec2-user** as a user name and the key-pair that is assigned at launch.

#### **NOTE**

All EC2 AWS Linux instances have the default account of ec2-user. If you launch another type of Linux instance, such as SuSE, Red Hat, or CentOS, the default accounts are different.

#### **Follow these steps:**

1. Log in to the UI and select **Credentials, Manage Targets, Accounts**.
2. Select **Add** to add an account.
3. In the **Application Name** field, select the magnifying glass and select **AWS Access Credential Accounts**.
4. For the **AWS Credential Type**, select **EC2 Private Key**, then enter values for the following settings:
  - **EC2 Instance User Name**
  - **EC2 Private Key**: Navigate to your **.pem** file and select **Upload**.
  - **Key Pair Name**: Name of the key pair you assigned in AWS Console, such as **cademo-key-pair**

### **Configure an AWS Connection to the Instance Region**

After you configure a credential account, add an AWS connection to the region in which your AWS instances are running.

#### **Follow these steps:**

1. From the UI, select **Configuration, 3rd Party, AWS**.
2. Select **Add**.  
The Add AWS Connection page opens.
3. Enter these values for the following fields:
  - **Access Key Alias**: cademo
  - **Region**: Select the region where your instances are running from the pull-down list.
  - **Active**: Select this checkbox to schedule this Alias/Region for import from AWS (at the frequency that is selected on the **Refresh Interval** tab).
4. Select **OK**.  
A confirmation window displays indicating that the AWS import is initiated.  
The Privileged Access Manager instance connects to the AWS Public API endpoint over port 443. Using the credentials in the vault, Privileged Access Manager tries to connect and start importing devices. If the connection is successful, a confirmation message displays.
5. Verify that the connection is listed in the Amazon Web Services (AWS) Configuration section.
6. (Optionally) Select **Test** to verify connectivity. After a successful test, the message "Connected successfully to AWS" displays.
7. (Optionally) To gain access to data centers in multiple regions where AWS is present, from the one connection panel, add other AWS regions. You then have access to these centers from the centralized single console.

### **Configure a Device Group for Access Policies**

Create a device group for use in an access policy for the AWS Management Console. These instructions are for AWS on Linux or Windows.

#### **Follow these steps:**

1. Log in to the Privileged Access Manager UI.
2. Select **Devices, Manage Device Groups**.
3. Select the Create Device Group link.
4. Set the following values:

**Group Name:** Enter a string. For example, AWSLinuxDevices or AWSWindowsDevices

This value must match the value that you specify for the Groups tag that you configure when launching an AWS instance later.

**Group Type:** AWS

**Access Methods:** SSH (Linux) or RDP (Windows)

5. Select **Save**.

### **Configure Session Recording Storage to Amazon S3 (Optional)**

You can store session recordings in an Amazon S3 bucket. If session recording is being done using CIFS/NFS, Amazon S3 is not necessary. This step is optional.

1. From the UI, select **Configuration, Logs, Session Recording**.
2. Select the **External Storage** tab.
3. In the **Primary Mount Settings** section, select Amazon S3 from the **Protocol** drop-down list.
4. Complete the remaining fields:
  - **Bucket** - Enter the AWS bucket to use.
  - **AWS Provision**- Select the appropriate entry from the drop-down list.
5. Select **SAVE SETTINGS**.
6. A confirmation message appears at the top of the screen.
7. **Select Mount.**  
A message appears at the top of the page indicating whether the mount is successful.  
If the share is mounted, **Mount Availability** displays the status of the mount: **available** or unavailable.
8. Go back to the **Session Recording** tab.
9. Specify the following types of sessions that you want to record:
  - **Text based recording to a NFS/CIFS/S3 mounted directory**
  - **Graphical session recording to a NFS/CIFS/S3 mounted directory**
 Each session recording option is unavailable until the required network mounts have been configured.
10. Select the **UPDATE** button to save your changes.  
If the configuration is successful, the message **Keystroke Logging configuration updated successfully** displays.

### **Define AWS User Access Policies (Optional)**

Privileged Access Manager provides two default AWS policies:

- IAMUserAccess
- PowerUserAccess

You can add your own user access policies. Select **Policy, Manage Policies, Create AWS Policy**.

### **Create an AWS Management Console Access Policy**

Create an access policy to the AWS Management Console. When an administrator accesses the AWS Management Console through Privileged Access Manager, the session is recorded, leaving an audit trail.

Configuring access eliminates the need for an AWS administrator to establish individual accounts with policies and permissions for each privileged user and associated applications. If you configure access for one account (cademo), you centralize access. However, logging and auditing is still tied to the user performing the action.

For auto-login, do not configure any AWS connections from the Configuration, 3rd Party menu. Simply load the access key and a secret access key into the Credential Manager account for each AWS instance that you want to manage.



**NOTE**

After you configure access to the AWS Console, only the permissions that are associated with the AWS IAM user are added for Privileged Access Manager. Earlier in this procedure, you assigned AmazonEC2ReadOnlyAccess policy to the IAM user so that user has read-only access to specific Amazon EC2 services and resources. For more information about AWS access permissions, see the AWS Directory Service user documentation.

**Follow these steps for access to the AWS console:**

1. From the UI, select **Policies, Manage Policies**.
2. Select **Add**.
3. In the User or User Group field, enter **super**.
4. In the Device or Device Group field, enter [xceedium.aws.amazon.com](https://xceedium.aws.amazon.com)
5. On the Services tab, select AWS Management Console SSO [AWS Access Credential Accounts – cademo – PowerUserAccess]
6. On the Recording tab, select **Web Portal** and **On Violation**.
7. Select **Save**.

**Create an Access Policy for the AWS Device Group**

For the Linux or Windows Device group, create an access policy that allows the super account access to the AWS instances. These procedures are similar to adding any access policy for an individual or group.

**Follow these steps:**

1. From the UI, select **Policies, Manage Policies**.
2. Select **Add**.
3. In the User or User Group field, enter **super**.
4. In the Device or Device Group field, enter the device group for your OS (AWSLinuxDevices or AWSWindowsDevices).
5. On the Access tab, select one of the following access methods:
  - **Linux:** SSH
  - **Windows:** RDP
6. On the Recording tab, select the relevant options:
  - **Linux:** Command Line, Bidirectional, On Violation
  - **Windows:** Graphical, On Violation
7. Select **Save**.

**Launch New AWS Instances (Optional)**

Typically, there are AWS instances that are already launched. If you want to launch any new instances, you access the AWS Management Console from the Privileged Access Manager Access page. From the Console, you can launch new instances. Accessing the Console using PAM lets you record and log the creation of the new AWS instances.

You created an AWS Management Console access policy in a previous procedure. Now, you can securely access the AWS Management Console.

**Follow these steps:**

1. Log in to the PAM UI.
2. Select **Access**.
3. Select the **AWS Management Console SSO** link. You are automatically signed in to the AWS Management Console.

Now you can launch new AWS instance. See the AWS documentation for how to [launch EC2 instances](#).

## Connect to AWS Instances

After all AWS instances are launched, connect to any instance from the Access page of the PAM UI.

### Import the AWS Instances

After you finish the AWS configuration, import the AWS instances.

#### **Follow these steps:**

1. From the PAM UI, select **Devices, Manage Devices**.
2. Select **Refresh AWS Devices** link.
3. Ensure that you see all your AWS instances.

### Connect to an AWS Linux Instance Using Auto-login

Follow these steps:

1. From the UI, select **Access**.
2. Select the **SSH** Access Method link for an AWS Linux instance.  
You are connected automatically and logged in as a valid user with the AWS EC2 Private Key.

### Connect to an AWS Windows Instance

To connect to an AWS Windows instance from the Access page, you need the Administrator password. Retrieve this password from the AWS Management Console then you can access the instance.

#### ***Retrieve the Administrator Password for the Windows Instance***

For Amazon EC2 Windows instances, AWS generates and encrypts a random Administrator password using the certificate (public key) of an Amazon EC2 key/certificate pair. Retrieve the Windows instance password by using the AWS Management Console and then by providing the corresponding Amazon EC2 private key to decrypt the password.

#### **Follow these steps in the PAM UI:**

1. Select **Access**.
2. Select the **AWS Management Console SSO** link. You are automatically signed in to the AWS Management Console.
3. Navigate to **EC2 Dashboard, Instances**.
4. Right-click on an instance entry
5. Select **Get Windows Password** from the pop-up menu.  
The window **Retrieve Default Windows Administrator Password** opens.
6. In the middle of the page, select **Choose File** and navigate to the file on your local system with the private key file.  
Example: cademo-key-pair.pem

## Retrieve Default Windows Administrator Password



To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

**Key Name** cademo-key-pair

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

**Key Pair Path**  cademo-key-pair.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAiZarbQsrOoe9heGmCw8Wh79jORmxxwQx9mMs4DdxdiUqULXSpY/ZCoj6i8Xe
Qy7me05pOezuMjfaX5b9VBwQ5aQogFZw3jmPiO278hFyWWaR8qsA/mx5ayQuYQYq2t6bjauA9uou
gjitpUsiB0bbMkw4J/JYZXqLHTxhlwKSkauVhMXH+JUXf5xfsPxJDYjWNQ8Ettino3hCy6cP+FYdt
ljAqutVLbyJMw5R+eObPLrctvYbZiireRDERGjW0FncfzQJE+2pzHywuixV+7Jw2rw5ShR99QPLn
```

Cancel

Decrypt Password

### 7. Select **Decrypt Password**.

A second page displays with the Administrator credentials, including the password.

### 8. Copy the information to your local system then log out from the AWS Console.

### 9. Return to the **PAM UI**.

## Connect to the Windows Instance

### Follow these steps:

1. From the UI, select **Access**.
2. Select the **RDP** Access Method link for an AWS Windows instance.  
You are prompted to accept the remote computers certificate.
3. Select the box **Do not ask me again** then **click OK**.  
The login page appears.
4. Enter the credentials and the domain that you copied from the AWS Console then select **Login**.

## Deploy a VHD on Microsoft Azure

Complete all the procedures in this topic to deploy a Privileged Access Manager instance on Microsoft Azure.

### Obtain Prerequisite Items

Obtain the following prerequisite items:

- A subscription to Azure.
- A Privileged Access Manager Azure VHD (Privileged Access Manager rX.x for Azure.tgz , which you download from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

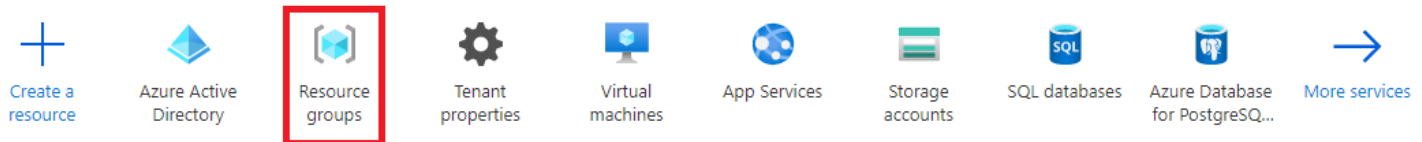
### Create a Resource Group

In Azure, a Resource Group is a logical folder for all the resources you create, including Disks, Storage Accounts, VMs, and Network Security Groups. If your organization limits the ability to manage Resource Groups, reach out to your Azure Administration Team for assistance.

To create a Resource Group, follow these steps:

1. Log into Azure with an account with permission to create a Resource Group.
2. In the Azure UI, select **Resource Groups** from the **Azure services** menu at the top of the screen (as shown highlighted in the following screen capture):

Azure services



vhd

3. Select the **+ Create a resource** button in the top left of the **Resource Groups** screen.
4. Complete the fields on the **Create a resource group** screen that opens.
5. Select **Review and create**.
6. Verify that the resource group information is correct and select **Create**.

### Create a Storage Account

To create a Storage Account, follow these steps:

1. Return to the Azure home screen and select **Storage Accounts** from the **Azure services** menu at the top of the screen.
2. Select the **+ Create** button in the top left of the **Storage accounts** screen that opens.
3. On the **Create Storage Account** screen, provide the following information:
  - For **Resource group**, select the drop-down menu and select the resource group that you created in the previous procedure.

#### TIP

If you do not see your resource group, you can search for it by typing in the **Select existing** field at the top of the list of existing resource groups.

- The **Storage account name**, which must be 3 to 24 characters long and contain only lowercase letters and numbers.
  - {Optional} Specify the **Location** of the storage account, which can be different from the location of the resource group.
4. Select **Review and create**.
  5. Verify that the storage information is correct and select **Create**.
  6. The storage account is deployed and added to the list on the **Home, Storage Accounts** screen.
  7. Select your new storage account from the list. You must select the **Refresh** button.
  8. Select **Containers** from the **Data Storage** section in the navigation rail to the left. The **Containers** pane opens.

9. Select **+ Container** to create a storage container in the storage account. A **New Container** panel opens on the right of the screen.
10. In the **New Container** panel, enter a **Name** for the new container and select **Create**

**NOTE**  
The container name can only contain lowercase letters, numbers, and hyphens, and must begin with a letter or a number. Each hyphen must be preceded and followed by a non-hyphen character. The name must also be from 3 through 63 characters long.
11. On the **Containers** panel, locate your new container and select its name (not the checkbox to its left).
12. In the panel that opens, select the **Upload** icon in the upper left then select the Privileged Access Manager VHD image to upload it to Azure.

### **Create a Network Security Group**

Next, create a Network Security Group in Azure.

#### **Follow these steps:**

1. Enter "Network Security Group" in the search field at the top of the Azure portal.
2. Select **Network Security Group**.
3. On the **Network Security Group** page that opens, select the **+ Create** button to add a new Network Security Group.
4. For **Resource Group**, select your Resource Group.
5. Provide a **Name** for the Network Security Group.
6. For **Region**, select the same location as your storage account.
7. Select **Review + Create**.
8. Select **Create**.
9. Once the deployment is complete, select **Go to resource**.
10. Select **Inbound security rules** on the left panel.
11. Select the **+ Add** button.
12. On the **Add inbound security rule** page that opens, add rules for ports that you want to open. See [Default Ports for Credential Manager](#) for more information about which ports to open.
13. Select the **Add** button to commit the changes and create the Network Security Group.

### **Create a Virtual Network**

Next, create a virtual network in Azure.

#### **Follow these steps:**

1. Enter **Virtual Network** in the search field at the top of the Azure portal.
2. Select **Virtual Networks**.
3. On the **Virtual Network** page that opens, select the **+ Create** button to add a new Virtual Network.
4. For **Resource Group**, select your Resource Group.
5. Provide a **Name** for the Virtual Network.
6. For **Region**, select the same location as your Storage Account.
7. Select **Review + Create**.
8. Select **Create**.
9. Once the deployment is complete, Select **Go to resource**.
10. Select **Subnets** on the left panel.
11. Select the subnet "default" to show its properties
12. In the **Network security group dropdown**, find and select the new Network Security Group that you created earlier.

**NOTE**

Do *not* use the default value "None."

13. Select **Save** to commit the change.

### **Create a Managed Disk**

Next, create a disk in Azure.

#### **Follow these steps:**

1. Enter "disks" in the search field at the top of the Azure portal.
2. Select **Disks** from the search results.
3. On the **Disks** page, select the **+ Create** button to add a new disk.
4. Under **Project Details**, select an existing **Resource Group** from the drop-down menu.
5. Under **Disk Details**, provide the following information:
  - The **Disk Name**.
  - For **Region**, select the same location as your **Storage Account**. You must create a disk in the same location as the storage account where you uploaded your VHD.
  - To specify the disk source type and properties, follow these steps:
    - a. Select "Storage blob" from the **Source Type** drop-down menu. More context-sensitive controls appear.
    - b. In the **Source blob** field, use the **Browse** link to select the VHD. Select the Storage Account, then the Container, then the VHD, and finally select **Select**.
    - c. For **OS type**, select "Linux."
    - d. Verify that the value of the **VM generation** control (which appeared when you select Linux in the previous step) is "Gen 1."
  - To change the default **Size** (1024 GiB) of the disk, do the following steps:
    - a. Select the **Change Size** link. The **Select a disk size** page opens.
    - b. Verify that the value that is specified in the **Disk SKU** drop-down menu is "Premium SSD".
    - c. Select a listed disk size or specify a **Custom disk size** of at least 80 GiB.
    - d. Select **OK**
6. Select **Review and Create**.
7. Verify that your settings are correct and, if so, select **Create**. Otherwise, select the **Previous** button to go back and make any necessary changes.

### **Create the Virtual Machine**

To create a Privileged Access Manager VM in Azure, follow these steps:

1. Return to the **Disks** page and select your disk. A new pane appears with **+ Create VM**.
2. Select **+ Create VM**. The **Create Virtual Machine** panel appears.
3. In the **Basics** tab, enter a **Name** for your VM.
4. For **Resource Group**, select "Use Existing" and select your Resource Group.
5. **Location** is disabled because it is determined by the disk Storage Account location.
6. Select a size. See [Installation Requirements](#) for more information. Select the size and then the select the **Select** button at the bottom.
7. Select the **Networking** setting and do the following steps:
  - a. Select the Virtual Network that was created earlier. The "default" subnet is selected.
  - b. On the **Public IP** drop-down list, select **Create New**.
  - c. On the **Create public IP address** page that opens, set the **SKU** option to "Standard."
  - d. On the **NIC network security group**, select **Advanced**.
  - e. On the **Configure network security group**, select the name of the Network Security Group that you created earlier.
8. Select **Review + Create**.

9. Verify the settings on the **Summary** page, then select **Create** to commit your changes.  
Deployment begins. To monitor its progress, select the **Notifications** bell icon in the upper right.

### **License Your Azure PAM Instance**

Once the VM deployment is complete, log into and license the Privileged Access Manager instance.

#### **Follow these steps:**

1. Select **Virtual Machines** on the left rail.
2. Select the VM that you created. The **Public IP Address** is listed in the right column of the **Overview** tab.
3. Use the public IP address to access Privileged Access Manager UI. For more information, see [Accessing PAM](#).

#### **NOTE**

If your initial attempt to access the PAM UI fails, try rebooting the new PAM instance.

4. Select **Configuration, Licensing**
5. Copy the Hardware ID.
6. Contact Broadcom Support and request a license file with Azure support for the instance that is identified by the Hardware ID. For more information, see [this KB article](#).
7. Once you have the license file, Do the following tasks to install the license it:
  - a. Navigate to the **Configuration, Licensing** page and select the **Install New License** tab.
  - b. Choose the appropriate license file and select **Upload file**.
  - c. Verify the new license and select **Save New License**.

#### **NOTE**

The Azure LinuxDiagnostic extension is not available for Privileged Access Manager.

### **Set up CIFS Storage in Azure**

You can set up Azure to store your session recordings and database backups on an Azure CIFS share. Alternately, you can use an on-premises CIFS or NFS share, or create a separate Linux device with an NFS share in Azure. Azure does not support mounting an Azure file share in a different region than your Azure Privileged Access Manager VM. Once you have a share, follow the instructions in [Schedule a Backup of the Database](#).

To create a CIFS share in Azure, follow these steps:

1. In Azure, select the **Storage Accounts** menu on the left.
2. Select your Storage Account.
3. Under **Services** in the right pane, select **Files**.  
The File Service window appears.
4. Select the **+ File Share** button on the top left of the **File Service** panel.
5. Enter a Name in lowercase characters and numbers. Hyphens are allowed.
6. Enter a **Quota** (size limit) in **GB**.
7. Select the new File Share. In the resulting right pane, select **Connect** from the top menu.
8. Scroll down to the **Connecting from Linux** section.
9. Copy the command from the text box. We are only interested in the share path, user name, and password. The following example highlights those three elements:

```
sudo mount -t cifs //mystorage.file.core.windows.net/myshare
[mount point] -o vers=3.0,
username=mystorage,
password=7QX+bNjogEd7vvvJERIKzcqVVqzOV3CLuqqNE6FacZCtiK1F7ZAA4BT11I48EfbBmaMnNWQCz8XYizuNvjtrIQ4=,
dir_mode=0777,file_mode=0777,sec=ntlmssp
```

This share uses the CIFS Protocol, and SMB version 3.0.



10. Use this information to set up:

- a. Session Recording: See [Set up Session Recording](#).
- b. Database Backup: See [Schedule a Backup of the Database](#)

#### NOTE

**Next step:**

- [Configure an Azure Connection](#)

## Configure an Azure Connection

An Azure Connection enables clustering, importing of Azure Virtual Machines, and using Azure Active Directory as a SAML Identity Provider. You configure Azure as a Target Application and a Target Account in Privileged Access Manager, and then configure a connection. If you only want to manage Azure AD accounts, and not devices, see [Add an Azure AD Target Connector](#) instead.

### Azure as Target Application

#### *Create the Application in Azure*

The Azure Application allows Privileged Access Manager to access Azure Resource Groups, VMs (for Azure device import), network interfaces, and public IPs (for clustering).

#### NOTE

For clustering, configure the Azure Application on the first Primary Site member. See [Set Up a Cluster](#) and [Cluster Deployment Requirements for Azure](#) for more information.

Your configuration differs depending on whether you plan to manage accounts, devices, or both. If you are only managing devices, you can use public APIs or a web connection. For information about required privileges, see the Microsoft Azure document [Administrator roles by admin task in Azure Active Directory](#).

### *Application Registration*

To create an Application in Azure, follow these steps:

1. In Azure, select **Azure Active Directory** from the left menu.
2. Select **App Registrations** from the resulting service list.
3. Select **+New Registration** on the resulting pane.
4. Enter a **Name** of your choice. Do not include spaces in the name.
5. Select **Supported Account Types**: Accounts in this organizational directory only.
6. Select **Redirect URI**:
  - Select **Web** if you want to discover and manage devices but not accounts. This option does not require your Azure account name and password.
  - Select **Public client (mobile & desktop)** to be able to discover and manage accounts and devices. This option requires your Azure account name and password. You can also use this option to manage devices only.
7. Enter a **Sign-on URL** for the application. Enter your Azure Privileged Access Manager URL. For a cluster, select the IP address of the first node at the primary site. For example: `https://ip_address/cspm/home`
8. Select **Create**.
9. Open the App.
10. Copy the **Application ID** for use in creating a Privileged Access Manager Target Account.
11. Select **Certificates and secrets** in the **Manage** menu.
12. Under **Client secrets**, select **+New client secret**. Enter a **Description**, and an **Expires** Duration.
13. Select **Add**.

The **Value** of the Secret key appears. Copy the key value now. You cannot retrieve it after you leave this page. You must use it as the **Secret Access Key** when you create the Target Account.



If you are only managing devices, and using the **Web** option, skip to [Add Application to Resource Group](#). If you are managing devices using the public client, go to the following section. If you are managing accounts using the public client, go to [Account Management Using Public Client](#).

### ***Device Management Using Public Client***

1. Open the App that you created.
2. In the **Manage** menu, select **API Permissions**.
3. On the API Permissions panel, select **+Add a permission**.
4. On the Request API Permissions page, select **Azure Service Management**.
5. Select **Delegated permissions**.
6. Under **Select permissions**, type to search for "directory."
7. In the search results, select **user\_impersonation** (Access Azure Service Management as organization users (preview)).
8. Select **Add Permissions**.
9. Under **Grant consent**, select **Grant admin consent for [your directory]**.
10. Select **Yes**.
11. Close **API permissions**.
12. On the application **Manage** menu, select **Authentication**.
13. Scroll down to **Default client type**. Select **Yes**.
14. Select **Save**.
15. If you are not managing accounts, skip to [Add Application to Resource Group](#). If you are managing accounts, go to the following section.

### ***Account Management Using a Public Client***

1. Open the App that you created.
2. In the **Manage** menu, select **API Permissions**.
3. On the API Permissions panel, select **+Add a permission**.
4. On the Request API Permissions page, select **Microsoft Graph**.
5. Select **Delegated permissions**.
6. Under **Select permissions**, type to search for "directory."
7. In the search results, select **Directory.AccessAsUser.All** (Access directory as the signed in user).
8. Select **Add Permissions**.
9. Under **Grant consent**, select **Grant admin consent for [your directory]**.
10. Select **Yes**.
11. Close **API permissions**.
12. If you have not already set the Default client, go to the application **Manage** menu, and select **Authentication**.
13. Scroll down to **Default client type**. Select **Yes**.
14. Select **Save**.

### ***Add an Application to a Resource Group***

If you want to manage devices, you must associate your Application to your Resource Group:

1. Select **Resource Groups** from the Azure left menu.
2. Select your Resource Group.
3. Select **Access Control (IAM)**.
4. Select **+Add, Add role assignment**.
5. Select **Contributor** from the **Role** drop-down list. Leave **Assign Access to** as "Azure AD user, group, or service principal."
6. In the **Select** field, enter the name of your application. Select the application from the resulting list.

7. Select **Save**.

#### NOTE

If you have Virtual Machines in different Resource Groups (such as for clustering), repeat this association for each Resource Group.

### Create a Target Account

Clustering, Azure device import, and the Azure agent require a Target Account in Privileged Access Manager. Follow these steps in Privileged Access Manager:

1. Go to **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. Use the **Application Name** magnifying glass icon to search and select **Azure Access Credential Accounts**. This action populates **Host Name** and **Device Name** with **ca.portal.azure.com**.
4. Select the **Access Credential** tab.
5. Select the required **Azure Application Type** and then provide the appropriate credentials in the context-sensitive fields immediately below:
  - **Web App/API**:
    - **Account Name**: The application name that you created in Azure.
    - **Secret Access Key**: The password key for your Azure Application.
  - **Native Client**:
    - **User Name**: Your Azure account user name.
    - **Password**: Your Azure account password.
6. Enter the **Application ID** from your Azure Application. If you did not copy it earlier, follow these steps:
  - a. In Azure, select **More Services** from the bottom of the left menu.
  - b. Enter “enterprise” in the filter field, and select **Enterprise Applications**.
  - c. Select **All Applications** from the menu.
  - d. Select your application from the application list.
  - e. Select **Properties**.
  - f. Copy the **Application ID** GUID from the property page.
7. Enter the directory ID. Get the **Directory ID** from Azure. Follow these steps:
  - a. In Azure, select **Azure Active Directory** from the left menu.
  - b. Select **Properties** from its menu.
  - c. Select the **Directory ID** GUID from its property page.
8. Select the Azure Cloud type Azure Commercial Cloud or Azure US Government. Azure US Government is used by all government agencies. Any PAM instance that is deployed on behalf of the US government requires the Azure US Government cloud type.
9. Accept or changes any other fields as appropriate.
10. Select **OK** to save the Target Account.

### Add an Azure Connection

After you configure your Target Account, configure Azure as a third-party connection in Privileged Access Manager. Follow these steps:

1. Go to **Configuration, 3rd Party, Azure**.
2. Select **Add** on the Azure Configured Connections tab.
3. For **Account**, select the Azure account you created, using the magnifying glass icon.
4. Select your **Subscription ID** from the drop-down list.
5. Select your **Resource Group** from the drop-down list.

6. Select **Sync Virtual Machines** to synchronize Azure Virtual Machines to Privileged Access Manager.
7. Select **Sync SAML Users** to synchronize Azure SAML users to Privileged Access Manager.
8. Select **OK** to save the Azure Connection.
9. Select your new connection from the list and select the **Test** button.

**NOTE**

The SAML **Test** button only works when the IDP has a SSL/TLS certificate that has been signed by a Certificate Authority. The **Test** button fails if the IDP only has a self-signed certificate.

A confirmation message or an error appears above the list.

10. (Optional) Select the **Refresh Interval** tab to set the frequency of the download of information from Azure. You set separate intervals for SAML Users and Virtual Machines. The intervals default to 60 minutes, but can also be set to 5, 15, or 30 minutes.  
To refresh Virtual Machines immediately, use the **Refresh Azure Devices** button on the **Devices, Manage Devices** page.  
To refresh SAML Users immediately, use the **Refresh Azure SAML Users** button on the **Users, Manage Users** page.

**NOTE**

The **Refresh Azure SAML Users** button only appears when [Azure AD as an Identity Provider \(IdP\)](#) is configured. Likewise, the **Sync SAML Users** checkbox has no effect until Azure is configured as an IdP.

**NOTE**

- [Cluster Deployment Requirements for Azure](#)
- [Azure AD as an Identity Provider \(IdP\)](#)
- [Add an Azure AD Target Connector](#)

## Clone a PAM Server Instance on VMware, AWS, or Azure

This content describes how to clone a PAM server instance. Failure to follow these procedures can cause conflicts between the clone and the original server upon which it was based.

### Clone a VMware PAM Server Instance

Use this procedure to clone a VMware PAM server instance.

#### **Follow these steps:**

1. If the donor server instance is part of a cluster, remove it from the cluster until all cloning operations are completed.

**NOTE**

Failure to remove the donor server instance from the cluster can cause the new clone to replicate on behalf of the original the first time it is started. This issue can result in clustering errors (for instance, when the original server instance is started back up again),

2. After the donor server instance has been removed from any cluster, shut down PAM on that server instance to avoid a live snapshot becoming the source of a clone. Leave the server shut down until new IP addresses have been assigned to the clone, so that they do not clash with each other.
3. Use the standard VMware procedure to clone the donor server instance to a new one. Assign *new* MAC addresses to the network interfaces in the process.
4. Verify that the donor server instance is still shut down then start the clone server instance.
5. Assign a new host name and IP addresses to the clone.
6. Once the clone server instance has been restarted with a new IP address, start the donor server instance back up and rejoin it to a cluster if desired.
7. Reset the database on the new clone.

## Clone an AWS PAM Server Instance

Use this procedure to clone an AWS PAM server instance.

### Follow these steps

1. If the donor server instance is part of a cluster, remove it from the cluster until all cloning operations are completed.  
**NOTE**  
 Failure to remove the donor server instance from the cluster can cause the new clone to replicate on behalf of the original the first time it is started. This problem can result in clustering errors (for instance, when the original server instance is started back up again),
2. After the donor server instance has been removed from any cluster, shut down PAM on that server instance to avoid a live snapshot becoming the source of a clone. Leave PAM shut down until new IP addresses have been assigned to the clone, so that they do not clash with each other.
3. Use the AWS Management Console to create an instance from the original donor server instance.
4. Once the cloned server instance is ready, start it up.
5. Restart the donor instance and rejoin it to a cluster, if appropriate.
6. Reset the database on the new clone.

## Clone an Azure PAM Server Instance

Azure does not support cloning as such. Instead, you convert an instance to a template and then use that template as the basis for new instances.

### NOTE

When you convert an instance to a template, verify that you first remove it from a cluster if it belongs to one.



## Deploy the Hardware Appliance





The following topics provide information about the Lanner 404L hardware appliance, and instructions on how to install it:

No software installation is required on the appliance.

### Unpack the Hardware Appliance from the Packaging

The hardware appliance package contains, at minimum, the items identified in the following table. If any of these items are missing, contact Broadcom Support.

Item		404L (Dual Power Supply model)	
No.	Name	Quantity	Illustrations / Notes
1.	L-shaped brackets	4	
2.	Sliding rail assemblies	2	Each sliding rail assembly can be separated into an inner frame and an outer frame assembly. 

2a.	Inner rail frame	1 per sliding rail assembly	The inner frame (or inner rail) has an outer safety lock (see step 2c.) for securing it to the appliance.
2b.	Outer rail frame assembly	1 per sliding rail assembly	The outer frame assembly consists of two heavy-gauge rail frames (center rail and outer rail) that incorporate a ball-bearing slide. One frame attaches and allows extension of the two frames. The other frame allows extension of the inner rail frame with the center rail. The rail assembly has an inner rail frame that, with two L-shaped brackets, is attached to the rack.
3.	Short flat-head screws	8	
4a.	Long flat-head screws	8	
4b.	Nuts for long flat-head screws	8	
5a.	Flat countersink screws	12	
5b.	Conical washers for flat countersink screws	12	
6a.	Front ear brackets	2	
6b.	Ear bracket screws	6	
7.	Appliance chassis	1	

8.	Power cords	2	
9a.	Console cable	1	
9b.	Ethernet patch cord	1	

### **Mount the Hardware Appliance in a Rack**

With the provided equipment, you can mount the appliance into a standard rack.

1. Remove the two rail assemblies from their packaging.



*Model 404L rail assembly, inner side up*

2. Separate the inner rail frame from the outer and center rail frames on each of the two assemblies:
  - a. Place one rail assembly as shown:



*Model 404L closed frame assembly, inner side up*

- b. Slide the inner rail frame all the way to the left. The frame stops at about half its length:



*Model 404L inner rail extended to left, inner side up*

- c. Turn the assembly upside down so that its outer side is visible as shown here:





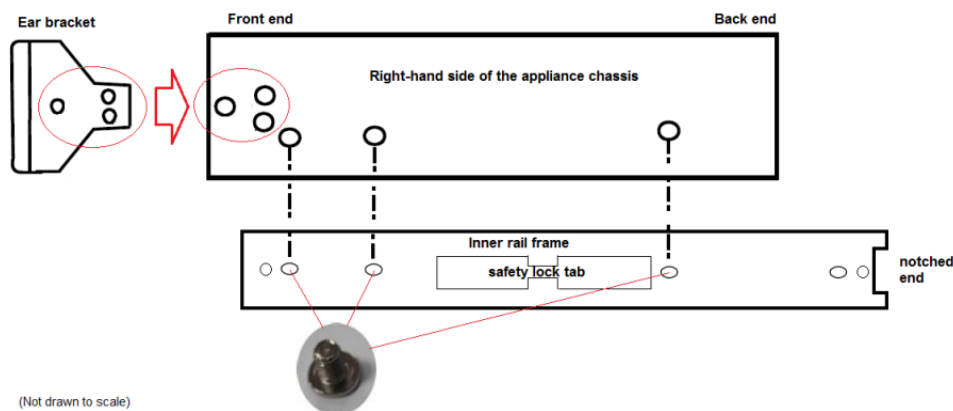
*Model 404L inner rail that is extended to left, outer side up, with arrow*

- d. Press down the outer safety lock tab (indicated by the arrow), and – holding the tab down – pull the inner rail frame firmly to the left so that it is removed.



*Model 404L separation of inner and outer rail*

- e. Repeat this inner rail frame separation with the other rail assembly.
3. Attach the inner rail frames and ear brackets to the appliance chassis
  - a. Align the three indicated mounting holes of the inner rail to the screw holes on the chassis frame with the outer safety lock tab facing out and the notched end of the rail that is located at the rear of the unit. (These are connected by vertical dashed lines in the figure.) Attach it to the appliance using three of the short flat-head screws.
  - b. Attach one of the two front ear brackets to the chassis using the small black screws provided in the ear bracket package.  
The two attached parts should now appear as in this diagram:
  - c. Repeat these steps to attach the other inner rail and front ear bracket to the other side.



*Model 404L inner rail and Ear bracket attachment to appliance chassis*



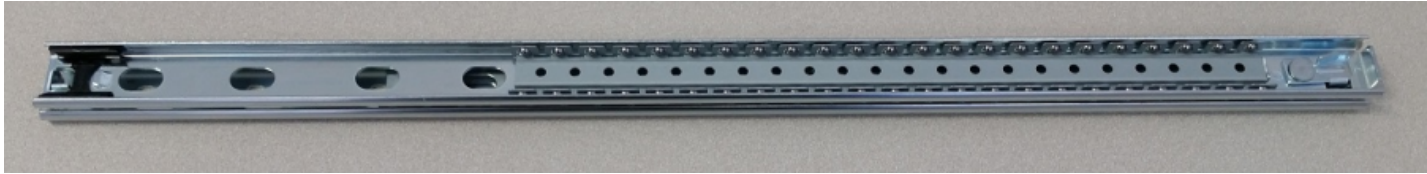
*Model 404L ear bracket and inner rail frame mounted on the right side of appliance*

The L-shaped brackets secure the outer rail frame assembly to the rack. Attach these brackets to the outer rail assemblies first, before attaching the combination to the rack.

4. Attach two L-shaped brackets to each of the two outer frame assemblies:

a. On one outer rail assembly, attach an L-shaped bracket at each end:

**Front bracket:** Close the outer rail assembly so that the center rail frame is lined up or flush with the outer rail frame. Slide the inner ball bearing assembly all the way to the right to expose four oval holes on the left.



*Model 404L outer rail assembly closed, inner side facing up, with ball bearing assembly slid to right.*

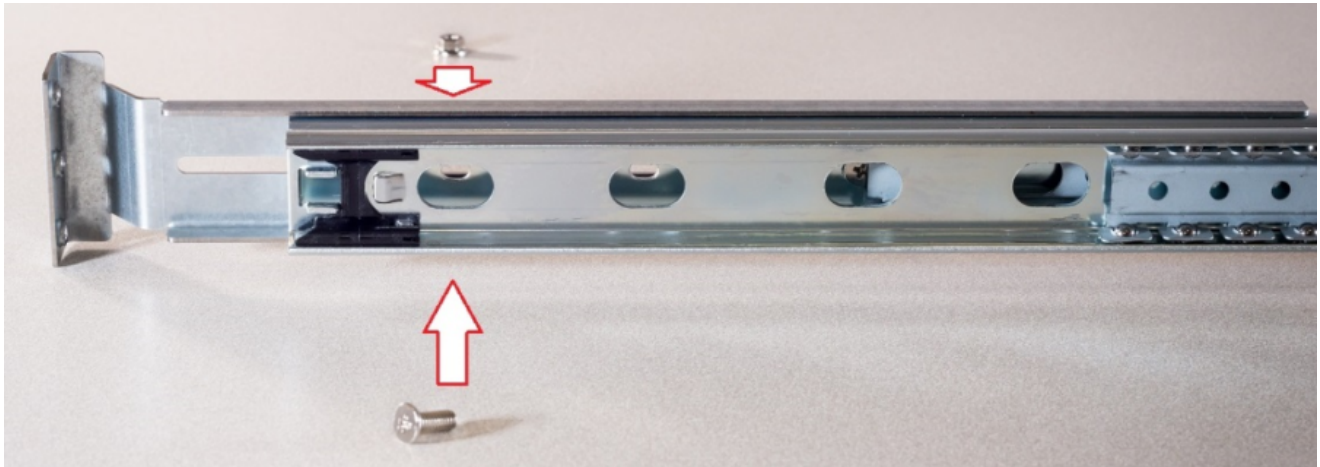
Locate an L-shaped bracket so that the curved edge on the bracket wraps around the outer rail assembly outer frame (when held up on its side edge as shown), and the left end of the bracket points down toward you.



*Model 404L: Orientation of the L-shaped bracket against outer rail assembly*

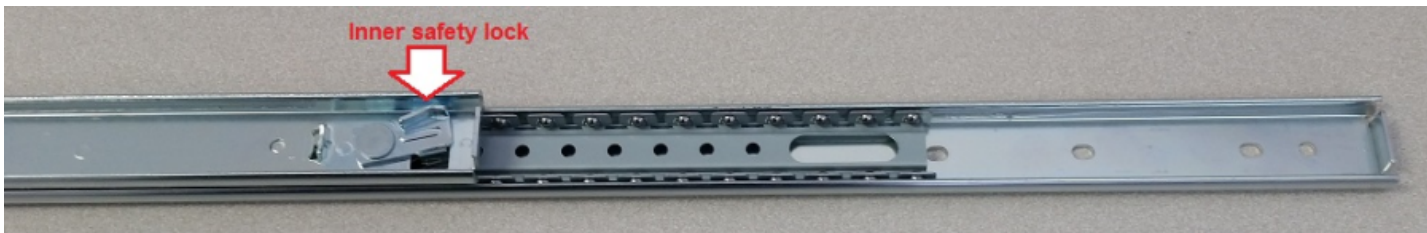
Insert a long flat head screw (see Package Contents Table, Item 4a) through the first oval hole on the inner frame of the frame assembly, through to the outer frame, then through the L-shaped bracket long groove, and finally attach (but not tighten) a nut (see Package Contents Table, Item 4b) to the end of the screw. Repeat this with a second screw and nut through another pair of rail holes. (The third or fourth hole pair provides the best support. The additional two hole pairs are intended for alternative equipment that is not used here.)

Do not tighten the nuts yet because you need to adjust the location of the brackets when you mount the bracket-rail assembly to the rack.



*Model 404L: Front bracket onto outer rail assembly, inner side view, with screw and nut before attachment*

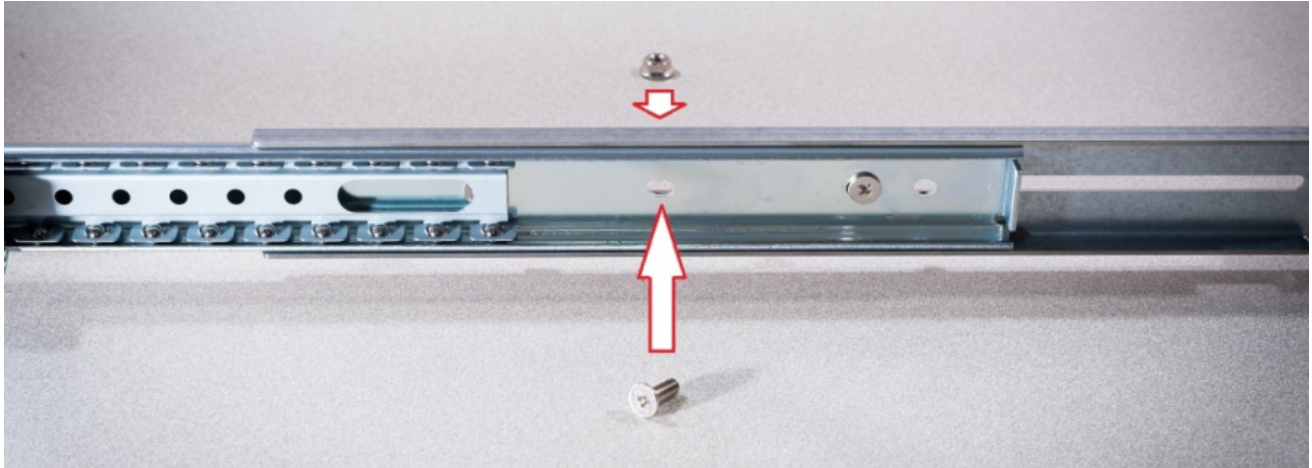
**Rear bracket:** Slide the outer rail away all the way to the right so that the inner safety lock snaps in place, exposing the screw holes on the outer rail:





*Model 404L: Outer rail assembly after sliding the outer rail (on the bottom side) to the right*

Attach the second L-shaped bracket to the other end of the outer rail with two long flat head screws, one through the first or second oval hole (Figure 176) from the center, and one through the third oval hole near the end.



*Model 404L: Rear bracket onto left outer rail assembly, inner side view, with screw and nut before attachment*

- b. Repeat these steps to attach the other two L-shaped brackets to the other outer rail assembly. When you turn the assembly around so that its outer edge faces you, it should appear with the brackets loosely mounted (for now):



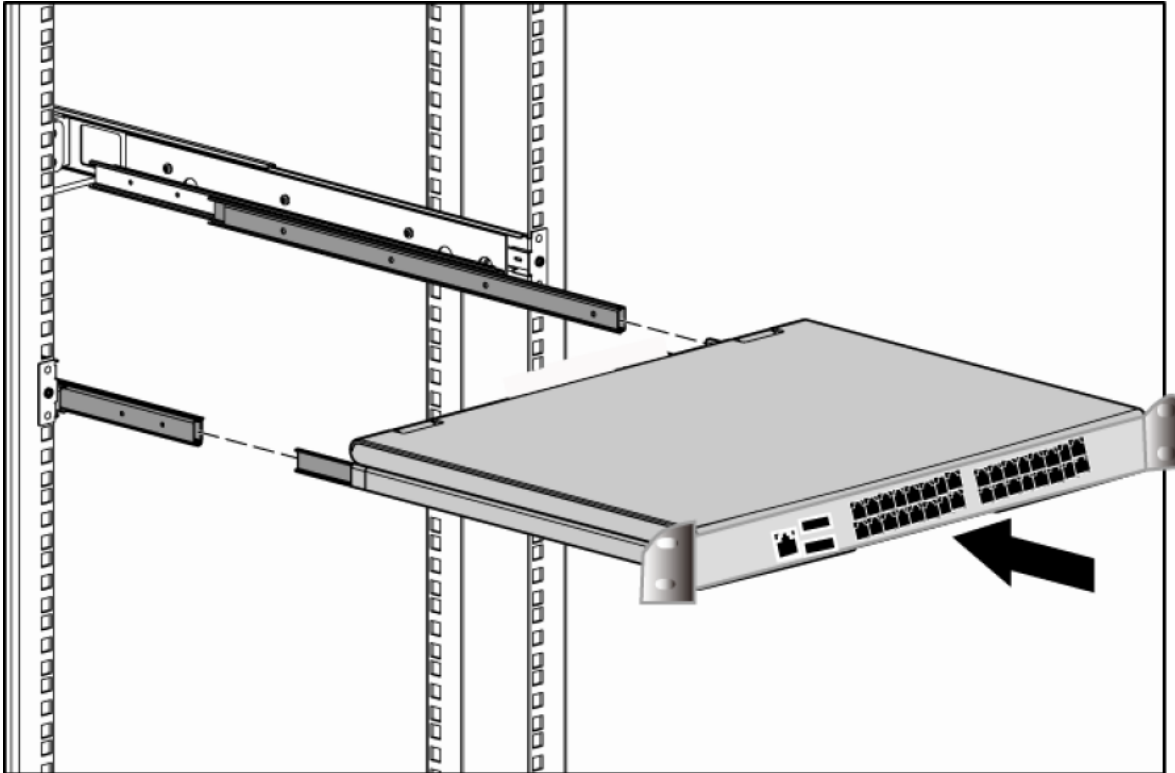
*Model 404L: Outer and center rails with brackets (loosely) attached (Step 4), front at left, outer side view*

5. Mount each bracket-rail assembly to the rack in an appropriate rack bay:
  - a. Install the outer rail with the attached bracket to the front rack post by using two countersink screws and, if the rack holes are not pre-threaded (which might require clips), the conical washers provided. Note that the front end of the rail assembly has a black plastic H-shaped component.
  - b. Extend and adjust the rear bracket to meet the depth of the rack and secure it to the rack post with two countersink screws and conical washers.
  - c. Repeat steps (a) and (b) above to install the other rail to the other side of the rack.
  - d. You can now use a wrench to tighten the nuts and the screws that attach the L-shaped brackets to each of the rails.



*Model 404L: Right side rail, with the front bracket attached, mounted at the front right side of rack*

6. Place the appliance (with ear brackets and inner rails attached) in the rack, as shown here:



*Model 404L: Placing the appliance into the rack*

7. Slide the appliance into the frame. As you do, hold the tabs on the outer safety locks (as in 2.d.) on the left and right sides of the appliance, so that the appliance can slide all the way in, while the attached inner rails are prevented from sliding back out.
8. Attach the ear brackets to the frame through their remaining (center) holes.
9. Connect the Ethernet patch cable to an Ethernet port on the front panel (example: port **1**, which corresponds to **GB1** in the LCD and GUI interfaces), and to the network.
10. Connect the power cords to the two PSUs and to outlets.

### **Configure Network Connections for the Appliance**

After the appliance is installed and optionally, mounted in a rack, [Configure Network Connections for the Appliance](#).

### **Appliance Power Supply Units**

Each power supply is a modular unit that slides out of the appliance for offline replacement or repair. The power supplies are held in place by release levers that are easily accessible when facing the rear of the appliance. Each power supply unit (PSU) uses a standard detachable power cord.

If the power supplied to the appliance is interrupted (power fails or a supply unit is removed or unseated), the unit sounds a steady alarm tone. This alarm continues until the **silence switch** turns off the alarm.

The silence switch is a small button at the back of the unit, immediately to the left of the power supplies. Press the silence switch to turn off the alarm. After the switch is pressed, it is reset only after the power is restored and recycled back to each appliance. Power restoration means that each power supply is seated in the appliance, and that each power cord is plugged in to a live power outlet.

## Hardware Appliance Specifications

The Dual Power Supply Model 404L hardware appliance provides redundant modular power support to promote continuous uptime. The hardware appliance can host any supported PAM release and has the following specifications:

Item	Description
<b>System components</b>	
Chassis	1U IPC
Power Supply	Redundant dual hot-swappable 300-W Power Supply Units (PSUs)
System Board	Intel C236 Chipset (Skylake PCH)
CPU	Intel Xeon E3-1275v6 processor Quad core (8 threads)
Memory	64-GB DDR4 2400MHz DIMM with ECC support
Primary Storage	240-GB Solid-State Drive (SSD)
Secondary Storage (Backup)	240-GB Solid-State Drive (SSD)
Display	2 line x 20 character LCD
<b>Standard interfaces</b>	
Network	Eight (8) 1-Gigabit Ethernet Ports
LCD inputs	Four-button control
Serial	One RJ-45 Console Serial Port
USB ports	Not functional
<b>Physical specifications</b>	
Height	1.73" (44 mm)
Width	17.2" (438 mm)
Depth	18.4" (468 mm)
Unit Weight	15.4 lb (7 kg)
Enclosure	Fits standard 19" rack
<b>Environmental specifications</b>	
Storage Environment	-20 Celsius to 70 Celsius 5 - 95 percent RH, noncondensing
Operating Environment	0 Celsius to 40 Celsius 5 - 90 percent RH, noncondensing
Cooling	Processor: Passive heatsink System: 3x cooling fan

## Configure Network Connections for the Appliance

After you set up the hardware appliance, configure the IP network interfaces so the appliance can access a network. You can set up your network connections using the LCD panel, the PAM UI, or a Console port. The appliance is inaccessible to the network until its IP address is assigned.

### Use the LCD Panel to Configure Network Connections

The LCD panel on the front of the appliance provides the interfaces to complete the initial hardware setup and network configuration. The LCD panel is a two-line, 16-character-per-line LCD display.

**TIP**

To connect to a device that cannot auto-negotiate speed or the duplex mode such as older switches and hubs, use the UI.

**Using the LCD Panel Menu**

Familiarize yourself with the LCD Menu on the front of the hardware appliance. The menu allows for basic network configuration of the device.

The LCD Menu Control has four buttons under the LCD Menu Panel, from left to right: < ^ v >. These buttons function as follows:

Button	Functions
< (left arrow)	<ul style="list-style-type: none"> <li>Move Left</li> <li>Undo/Cancel</li> </ul>
> (right arrow)	<ul style="list-style-type: none"> <li>Move Right</li> <li>Enter/Confirm</li> </ul>
^ (up arrow)	<ul style="list-style-type: none"> <li>Move up</li> <li>Increase value</li> </ul>
v (down arrow)	<ul style="list-style-type: none"> <li>Move down</li> <li>Decrease value</li> </ul>

**NOTE**

Older hardware appliances have an ENTER and an ESC button instead of the left and right arrows. Use the ENTER button to move right or to confirm an entry. Use the ESC button to move left or undo an entry.

The LCD menu includes the following options to operate the appliance:

**Network Setup**

This option allows the installer to provide the required network configuration to get the appliance operational. Use the Up or the Down arrows to navigate through the menu.

Menu item 1:	Network Setup
--------------	---------------

**Reset Password**

This option resets the configuration password to the default password. Select the left arrow and the password is reset. A message displays after a successful reset.

Menu item 2:	Reset Password	After selecting >:	Password reset!	After about 30 seconds:	Reset Password
--------------	----------------	--------------------	-----------------	-------------------------	----------------

**Reboot**

This option reboots the appliance. After you power down and restart the appliance, the LCD displays the Network Setup screen.

Menu item 3:	Reboot	After selecting >:	Rebooting...	After about 60 seconds:	Shuts down, Boots up
--------------	--------	--------------------	--------------	-------------------------	----------------------

**Power Off**

This option turns off the power, displaying the following message:

Menu item 4:	Poweroff	After selecting >:	Powering off...	After about 30 seconds:	Shuts down
--------------	----------	--------------------	-----------------	-------------------------	------------

The power switch remains in the "on" position, but you can switch it off.

### Halt

The **Halt** command stops all processes. The power is still on, but the device is unusable because all processes are stopped. The LCD has the following display:

Menu item 5:	Halt	After selecting >:	Halted.	After about 15 seconds:	Shuts down
--------------	------	--------------------	---------	-------------------------	------------

Use the Halt command when the power must remain on. For example, if a monitoring system raises alarms due to power loss, use Halt.

### Turn On FIPS

This option turns on FIPS mode. FIPS mode is fully compatible with PKI smartcard use, including the US DoD CAC system.

The LCD Menu option turns on the FIPS flag and reboots the appliance when it switches to FIPS mode.

- Use FIPS mode only when applicable. After the FIPS mode is activated, the LCD is no longer available for configuration. Use the UI to make all subsequent changes.
- To operate with socket filters in FIPS mode, the monitored devices must have release 2.7 or later Socket Filter Agents (SFAs).
- If for any reason FIPS activation fails, the LCD displays: PATCH FAILED / UPGRADE ABORTED. If this failure happens, the appliance cannot be revalidated until after it is returned to CA Technologies.

Menu item 7 (if set):	Turn on FIPS	After selecting >:	[several process messages]	Reboot ->	in FIPS mode
-----------------------	--------------	--------------------	----------------------------	-----------	--------------

### Basic Network Configuration Using the LCD Panel

After the appliance powers up, perform the basic network configuration using the menu on the LCD panel. The following steps assume that you have installed the appliance.

#### Follow these steps:

1. Connect the desired number of Ethernet cable connections to ports 1 through 8 on the appliance. These ports correspond to GB1 through GB8 in the LCD and UI interfaces.
2. Connect the power cord, first to the appliance and then to an outlet.
3. Power up the appliance:
  - a. Turn on the power switch on the back of the appliance. Hold the switch until the unit powers on.
  - b. Verify that the LCD is lit, indicating power.

During power-up, the menu cycles through several message screens until boot is complete.
4. Navigate to the **Network Setup** menu item on the screen, and press the right arrow (>).

The first screen is the **Default Gateway**:

```
Default Gateway
000.000.000.000
```

5. To configure the Default Gateway IP address, set the value of a digit for each digit position in the address. Use the up and down arrows to go through and select an integer from 0 to 9. Move to the other positions in the IP address using the > (forward) or < (backward) arrows. Complete this process for each address you want to configure. Each octet is expressed on the display using three digits. For each octet that is less than 100, the first characters are zero. For example, the address 10.44.146.3 is expressed in the LCD as 010.044.146.003

#### NOTE

These settings are saved when the Save option later in the procedure. For the settings to take effect after saving, the appliance must first be rebooted.

6. After you have set the last position in the IP address, press > to go to the next screen Interface Setup. To cancel the Network Setup and return to the Network Setup menu, press the left arrow.
7. Press > to go to the **Pick Interface** screen. This screen shows the interface available for configuration.
  - a. Use the arrows to select the label GB1 through GB8 corresponding to the label of the desired Ethernet port (1 through 8).
  - b. Use the up and down arrows to go through and select an integer from 0 to 9
  - c. Press > to set the IP address for the selected interface.
8. After setting the interface, enter the netmask for the same interface, on the **Netmask for GBn** screen.
9. At the final Interface Setup screen, enter one of the following options. Use the up and down arrows to position the arrow on the option and press > to enter this selection.

```
Interface Setup
Cont/Sav/eXit C
```

- Select **Cont** (Continue) to repeat the procedure for another interface.
- Select **Sav** (Save) to save your configuration.
- Select **X** (exit) to discard all network settings that you configured after the last save and restore the previous settings.

The LCD returns to the Network Setup display.

10. From Network Setup, navigate to **Reboot**, and press the forward arrow (>).

The appliance reboots and it is ready for configuration.

### Use the UI to Configure the Network Connections

An alternative to the LCD panel for network setup is the PAM UI. If your device is unable to auto-negotiate speed or the duplex mode, use the UI to configure the network connection.

The following steps assume that you have installed the appliance.

#### Follow these steps:

1. Configure a PC with a static IP address of: 192.168.98.x, where x is not 100. The IP address of GB1 as shipped is 192.168.98.100.
2. Connect this PC directly to the **1** port on the front of the appliance. Port 1 corresponds to **GB1** in the UI. This port is auto-sensing, so you do not need a crossover if using a laptop with the same.
3. Open a Java-enabled browser and enter the following URL, including the slash at the end  
<https://192.168.98.100/config/>  
 The trailing address slash is required.
4. Log in to the UI:
  - a. Accept the license
  - b. In the Windows Security pop-up window which follows, enter the default configuration username/password (config/config)
 The **Configuration, Network Settings** page appears.
5. Set the appropriate values in the **Network Settings** and **Network Interfaces** sections.



6. (Optional) Speed autosensing does not work with all network appliances. If you experience connectivity issues, set the **Speed** and **Duplex** settings to static values for the network interfaces.
7. Click **Update** when you are finished configuring the settings.
8. Click **Restart Networking** to commit your changes. While the network is restarting, the appliance is temporarily unavailable.
9. After the browser refreshes, use the Toolbar: **Logout** button (in the upper-right corner) to end your session.
10. Confirm that your settings have been correctly configured by accessing the login page using your newly assigned address.

### **Use the Console Port to Configure Network Connections**

If you cannot use the LCD Panel or the UI, use the Console port. The Console port is above the nonfunctional USB ports. This port enables you to connect the appliance to a monitor. A console cable is supplied.

Note the following port specifications:

- Speed: **115200**
- Data bits: **8**
- Stop bits: **1**
- Parity: **none**
- Flow control: **XON/XOFF**

## **Deploy the PAM Client**

The PAM Client is a fully functional alternative to the Web browser UI. Use the Client to access Privileged Access Manager and perform administrator and end-user activities. The Client eliminates the need to keep browser configurations compatible with the product. The Client does not interfere with browser-based UI access – you can use both methods from the same workstation. See [Supported Environments](#) for information about where you can run the PAM Client.

Complete the following procedures to deploy the Client.

### **Download the Client Software**

Download a client version compatible with your workstation OS type from the browser-based UI login page. To install the PAM Client, the user needs the same user rights or permissions as any other application that you install.

#### **Follow these steps:**

1. From your client workstation, open a browser and navigate to the URL of a PAM server using *one* of the following formats:

`https://server_ip_address/`

`https://fqdn_of_server`

where `server_ip_address` or `fqdn_of_server` is the system where you installed the PAM server.

#### **NOTE**

If you enter an IPv6 address, make sure to enclose the address in brackets. For example:

`[2001:db8:3333:4444:5555:6666:7777:8888]`

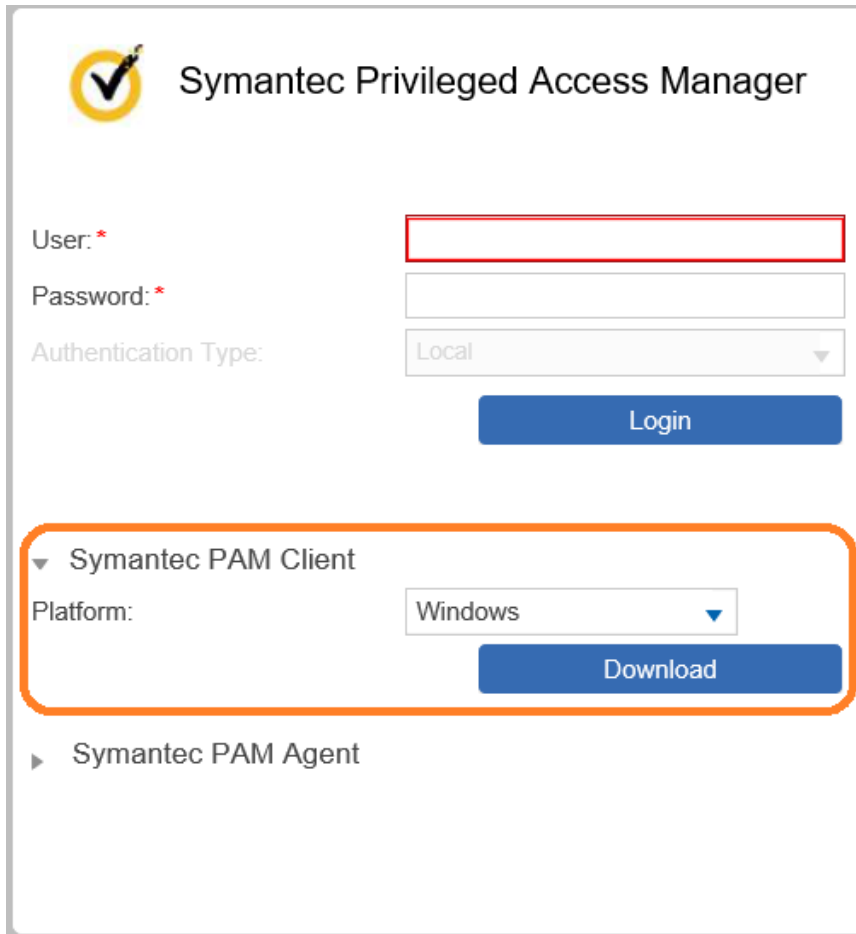
Examples:


– IPv4: `https://102.200.11.222/`

– IPv6: `https://[2001:db8:3333:4444:5555:6666:7777:8888]/`

– FQDN: `https://capam.forwardinc.com`

2. When the PAM UI login screen opens, select the arrow next to **Symantec PAM Client**. Context-sensitive controls open as highlighted in the following screen capture:



 Symantec Privileged Access Manager

User: \*

Password: \*

Authentication Type: Local

▼ Symantec PAM Client

Platform: Windows

► Symantec PAM Agent

3. In the **Platform** field, select the OS for your local workstation then select **Download**.
4. Save the installer file locally to your workstation.

### **Install the Client**

Refer to the appropriate instructions:

- [Specific macOS Instructions](#)
- [General Instructions](#)

### **Specific macOS Instructions**

After you download the installer file, extract the file and run the Client installer.

#### ***Use Sudo to Install***

For macOS, you can optionally use `sudo` to launch the installation. The installed files are then owned by `root`, preventing standard users from modifying the installed application files. With `root` ownership of the files, multiple users can concurrently use the same client installation. Use the following `sudo` command for `root` ownership:

```
sudo ./CAPAMClientInstall.app/Contents/MacOS/CAPAMClientInstall
```

The command "`sudo open CAPAMClientInstall.app`" does not give the ownership of the files to `root`.



If you install as `sudo`, the administrator password is only needed by during installation. However, if you do not install using `sudo`, you will only need the administrator password at run-time to use the SSH Proxy or SFTP Proxy. Everything other than the SSH Proxy or SFTP Proxy works without the administrator password.

#### NOTE

Sudo access is only necessary during installation. To distribute the PAM Client without user intervention, see the following:

- [Configure How the Client is Made Available](#)
- [PAM Client Silent Install](#)

PAM Client is a native macOS app with its own icon that appears in the dock.

#### NOTE

To log in to a PAM appliance from a macOS PAM Client, add the user certificate to the login keychain and system keychain. Adding the certificate prevents the user from being repeatedly prompted for login credentials.

### Multiple macOS Instances

To open multiple instances of the macOS PAM Client, invoke the binary `/Applications/CA PAM Client.app/Contents/MacOS/CAPAMClient` directly or use this command from terminal: `"open -n /Applications/CA\ PAM\ Client.app"`. Clicking the PAM Client app icon in Finder multiple times does not result in opening multiple instances.

### MacOS Subpixel Antialiasing

If you are using macOS Mojave with Subpixel Antialiasing disabled, the content in the Privileged Access Manager user interface may appear blurred. Re-enable Subpixel Antialiasing to fix this issue:

1. Open a Terminal.
2. Run the following command:

```
defaults write -g CGFontRenderingFontSmoothingDisabled -bool NO
```

3. Log out and log back in for the change to take effect.

### General Instructions

After you download the installer file, run the Client installer.

#### NOTE

If you install the Client in a UNIX environment, the UNIX system must have the necessary graphic libraries to show the PAM Client UI. Otherwise, when you run the Client, the Client exits without showing any error message in the log.

If the PAM Client starts, but the Dashboard Overview Tab is blank, the required libraries for the JxBrowser might be missing. To see which libraries are missing, go to the PAM Client installation folder and review the logs.log file. Install any missing libraries.

Follow the installation wizard, noting the following instructions:

- **License Agreement:** To accept the license agreement, scroll through the license text to the bottom of the panel.
- **Choose Install Set:** Select one of the following options:
  - **Typical:** Prompts you for an installation directory on your local workstation then installs the Client.
  - **Run:** Extracts the contents to a temporary location and runs the Client. The setup completes and the login screen appears.
- **Choose Install Folder:** Enter a path, or select the **Choose** button to find a folder. Consider the following options:

- If you use the default, ensure that the intended user has "Full control" of this folder. For example, a typical user might not have the required permissions to run the Client in the default folder.
- For a multi-user shared installation, select a directory where all users have write access. Another option is for each user to install the client separately in their own user folder, such as `c:\Users\<user>\`.
- For silent installation, see [PAM Client Silent Install](#).
- The PAM Client does not support installation in directories whose names include Japanese characters. If you install the PAM Client on a Japanese-language computer, enter a folder with no Japanese characters.

After the installation is complete, you can log in from the Client.

If you start the Client on a UNIX system and the UI Dashboard Overview Tab is blank, the libraries that the JxBrowser needs might be missing. To determine which libraries are missing, go to the Client installation folder and look at the `logs.log` file. This file lists the missing libraries are listed. Install those libraries.

### Log in from the Client

After the Client is installed, you can log in to the server. The initial client screen allows you to specify the address of a Privileged Access Manager appliance or appliance cluster VIP.

#### Follow these steps:

1. Open the client application.
2. Enter the following connection parameters for your server appliance.
  - **Address:** Enter the IP address in the form `address:port` or the assigned fully qualified domain name of the PAM server.

The PAM Client cannot use most well-known ports. See [Ports Not Allowed for the Client](#) for the full list.

#### NOTE

If you enter an IPv6 address, make sure to enclose the address in brackets. If you want to enter a port number with the IPv6 address, add a colon, followed by the port number. For example:

```
[2001:db8:3333:4444:5555:6666:7777:8888]:443
```

- **Connect Mode:** Select one of the following options:
  - **WEB:** Opens a connection to the server, and then opens a browser window to the UI. The console closes.
  - **CONNECT:** Opens a connection to the server, and displays a status connection console. The status connection console displays connection information and a **Launch Web Browser** and **Log Off** buttons.

You cannot switch between WEB and CONNECT, following your connection to the server. Select **Cancel** to return to the initial connection screen and restart the Client.
- 3. Select **Connect**.
- 4. If a client update is required, you are notified. Select **Update** to update automatically the installed client to the latest version. If necessary, restart the client.
- 5. If applet jars must be downloaded from the PAM server, you are notified. Select **Update** to install the appropriate applet jars automatically.
- 6. You may receive a **Verify Certificate** window before the login screen appears.
  - a. Select **View Certificate** to see the certificate details and evaluate its applicability.
  - b. If you approve of the certificate, select **Import** at the bottom of the dialog. Once it is trusted, you should not see the certificate warning any more.
- 7. When the login screen appears, enter the user name and password.
- 8. Select the **Authentication Type**.
- 9. Select **Login**.

Depending on the Connect Mode that you select, the browser window or the status connection window opens. If the status connection window opens, select **Launch Web Browser** to open the UI. The console window remains open. If you

close the browser window, you can Launch Web Browser later and can return to the same GUI location, as its state is preserved.

You can now use the product.

### **PAM Client Cache**

You can speed up the PAM Client connection to the Privileged Access Manager server by using the client cache. The cache saves reused files, much like any Web browser. The Client does not have a switch to turn the cache on or off. The cache works only if the Privileged Access Manager HTTPS certificate is configured properly. The certificate also must be trusted globally or in the local network or organization. The certificate cannot be trusted only by the client. Your whole system (OS) must trust the certificate. You can test whether your connection to the server is trusted by connecting with a Chrome browser. If you receive a Certificate warning such as "Your connection is not private," the cache is not used.

The PAM Client manages its own cache, but you may want to clear your PAM Client cache. To clear the PAM Client cache, delete this directory when all client processes have been terminated: `<client_root>\temp\web-cache`.

### **Modify Client Configuration Settings (Optional)**

The Client configuration settings specify operational behavior of the Client. Usually, the default Client configuration settings work for your environment. If necessary, you can modify the configuration settings.

#### **Follow these steps:**

1. From the Client login page, open the **Configuration Settings** window by selecting the gear icon in the lower-left corner
2. Select the relevant tab to change the following settings:

#### **Proxy**

##### **NOTE**

PAM only supports **Secure** (HTTPS) proxy.

Indicates whether the PAM Client is connecting to the PAM server through a proxy server. Select one of the following options for your deployment:

- No Proxy (default): The Client connects directly to the PAM server.
- Auto-detect proxy settings for this network: for a network-managed proxy
- Use system proxy settings: for workstation OS-managed proxy
- Manual system proxy configuration: for a custom target device as the proxy
- Automatic proxy configuration URL: for a web server-supplied proxy
- Ignore proxy certificate: This setting determines whether PAM trusts the proxy certificate. If the certificate is not trusted, the PAM Client cannot connect to the server. For security reasons, the setting is *unchecked* by default. If the Client keeps getting disconnected, it might be a result of a certificate mismatch. To avoid this problem, select this check box; however, this option is less secure.

#### **General**

Specifies memory for the Client.

- **Max memory size:** default (Windows, Linux x86): 1024 MB; (Mac, Linux x64): 2048 MB  
For Windows, 1200 is the maximum value. If the value is set to 1201 MB or greater, the client does not start again. If it does not restart, edit the **settings.properties** file at the installation root. Reset the **memory.max** parameter to 1200 or less and save the file.
- **Client language**  
By default, the Client automatically detects the language of the host computer OS and displays the user interface in that language, if available. To change the Client from the default to another language, clear the **Auto-detect** checkbox, and select a language from the **Client language** drop-down list.
- **Restore security prompts**

If you have previously selected a checkbox to ignore a security warning, selecting this **Restore** button causes the warnings to resume.

– **Use Host Address IP**

Set this option if PAM Client login attempts fail with "Unknown Error" messages.

**Cache**

Specifies the cache of previous PAM Client versions.

- **Enable Caching:** Stores previous versions for the PAM Client to revert to an earlier version. Default = On (checked).
- **Current Cache Size:** Specifies the total size of the cached versions of the PAM Client. Default: Total size of cached prior versions.
- **Clear Cache:** Specify to remove all cached versions. (You can remove individual versions by using the Manage button.)
- **Max Cache Size, MB (0 = unlimited):** Specify the maximum size of the cache by using the slider or the field.
- **Cached Versions:** Displays the number of cached versions.
- **Manage:** Displays details for all cached versions of the PAM Client. You can remove any or all versions.

**Certificate**

From a table list, specify a certificate authority (CA) certificate to be used. The PAM Client is provided with several preinstalled certificates. Add more if needed.

3. Select **OK** to save your settings.

**(Optional) Disable PAM Client Update Checking**

Use the following procedure to disable automatic update checking on PAM Clients that are experiencing startup issues.

**Follow these steps on each system on which a PAM Client is installed in your environment:**

1. Shut down any PAM Client instances that are running.
2. In the PAM Client installation folder, create a file called **update** with no file extension.
3. Open the **update** file with a text editor and entering the word `false`. Save and close the file.
4. Set permissions for the update file. For administrators, set full permissions. For users, set read-only permissions.
5. Launch the PAM Client and connect to the server.
6. If you see the message "Synchronization is Required," complete the following steps:
  - a. Select the gear icon in the left corner of the login dialog
  - b. Click Cache and select the following settings:
    - Enable Caching
    - Keep instances for reuse
  - c. Launch the PAM Client again and connect to the server.

**NOTE**

To re-enable update checking, delete the **update** file or edit it to remove the word `false`.

**Uninstall the Client**

**NOTE**

Starting from 4.1.3, the **CAPAMClient** binary and the **CAPAMClientInstaller** binaries are now 64-bit. The Java version for the PAM client has also been updated to use Java 17.

To use the latest PAM client, you as admin must either:

- Upgrade their existing PAM client to point to a 4.1.3 (or later) PAM instance,
- OR
- Use the installer to install the latest version of the PAM client.

If you choose to upgrade the existing PAM client to version 4.1.3, you cannot use the existing PAM client installer to uninstall this new version.

To uninstall the upgraded 4.1.3 PAM client, follow these steps:

1. Delete the PAM client installation folder.
2. Manually delete the registry key.

If you installed the PAM client as an administrator, delete the registry key in this location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Symantec PAM Client
```

If you installed the PAM client with credentials OTHER than an administrator, delete the registry key in this location:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Symantec PAM Client
```

If you choose to install the 4.1.3 or later PAM client, use the installer to uninstall as needed. You do not have to manually clean up the installation.

Follow the instructions for your workstation type:

### **Windows**

Do one of the following tasks to remove the Client:

- Remove the Client from the Windows **Control Panel, Programs and Features**.
- Remove a PAM Client installation from its location in the file directory:
  - a. At the root level of the installation, locate the directory `_/CA PAM Client_installation.`
  - b. Open this directory and run the uninstallation wizard named **Change PAM Client Installation**.

### **Mac**

To remove a Mac installation, you need root privileges. Delete the installation directory and its entire contents.

### **Linux**

To remove a Linux installation, delete the installation directory and its entire contents. Do *not* use the uninstallation wizard that is provided.

#### **NOTE**

Use the table of contents to access the other topics in this section.

## **Configure How the Client is Made Available**

The Client configuration settings reside on the Privileged Access Manager server. These settings determine whether the PAM Client is enabled and how the installer software is made available. By default, the Client is enabled and the installer is available on a CA Delivery Network internet-based CA Delivery Network (CDN) location.

Any user role with the Global Settings permission can modify the Client settings. Preconfigured user roles with the necessary permission include Configuration Manager, Global Setter, and Operational Administrator.

#### **NOTE**

To use the client, access to the client must be enabled. Enabling the download button to appear on the main login page is not sufficient to use the client.

**Follow these steps:**

1. Log in to the UI.
2. Select **Settings, Global Settings**.
3. Select the **Client Settings** tab.
4. Configure the following settings:

**Client Settings:** Accept the default, **Enabled** to use the client. **Disabled** allows only applet use.

**Distribution Method:** Determines how the client installer is downloaded. Select one:

- **Internet (CA Delivery Network):** Delivers the client installer and modules from the internet-based CA Delivery Network (CDN) location.
- **Intranet:** Delivers the client installer and modules from a server at the designated URL. Use this option only when the CDN is unavailable. Provide the FQDN or IP address of the download server using the text box.

**Download Button on Login Page:** Select the checkbox to make the client download buttons appear on the web UI login page.

5. Continue with the setup by deploying the client software.

## Symantec PAM Client Silent Install

You can create a silent installation process for your Symantec Client users.

### Silent Installation for Windows

To install the Symantec Client in silent mode on Windows, add the command line argument “-i silent”.

**For example:** CAPAMClientInstall\_V3.4.5.exe -i silent

You can customize installation arguments in an installer properties file. Create the file `installer.properties` and add the following strings:

```
# Installation mode (Silent)
INSTALLER_UI=SILENT
# Installation directory - use "\\" to separate directories.
USER_INSTALL_DIR=C:\\CAPAMClient
# Installation set (Complete/Upgrade)
CHOSEN_INSTALL_SET=Complete
```

Then, execute using “-f <path to installer.properties file>”.

**For example:** CAPAMClientInstall\_V3.4.5.exe -f installer.properties

### Silent Installation for Linux

To install Symantec Client in silent mode on Linux, you need the command line argument “-i silent”.

**For example:** ./CAPAMClientInstall\_V3.4.5.bin -i silent

You can customize installation arguments in an installer properties file. Create the file `installer.properties` and add the following strings:

```
# Installation mode (Silent)
INSTALLER_UI=SILENT
# Installation directory
USER_INSTALL_DIR=/opt/CAPAMClient
# Installation set (Complete/Upgrade)
CHOSEN_INSTALL_SET=Complete
```

To use the installer properties file, add “-f <path to installer.properties file>”.

**For example:** ./CAPAMClientInstall\_V3.4.5.bin -f installer.properties

## **Silent Installation for macOS X**

### ***Remote Silent Installation***

To install the Symantec Client remotely in silent mode on macOS X, use this command:

```
sudo ./CAPAMClientInstall.app/Contents/MacOS/CAPAMClientInstall -i silent
```

## **Symantec PAM Client Silent Uninstall**

Learn how to uninstall the PAM Client on UNIX and Windows.

Use the following procedures to silently uninstall the PAM Client on UNIX and Windows.

### **Silently Uninstall a PAM Client on UNIX**

Use the following procedure to uninstall a PAM Client on UNIX without displaying any indication of the process or requiring a reboot.

**Follow these steps to silently uninstall the *PAM 4.0 version or later* of the client:**

#### **NOTE**

Version 4.0 rebranded the product to Symantec, resulting in a change in the path.

1. Enter the following command:

```
./<Installation location of PAM client>\_Symantec\ PAM\ Client_installation\Change\  
Symantec\ PAM\ Client Installation -i silent -DUSER_REQUESTED_RESTART=NO
```

**Follow these steps to silently uninstall versions of the client *previous to PAM 4.0*:**

1. Enter the following command:

```
./<Installation location of PAM client>\_CA\ PAM\ Client_installation\Change\ CA\ PAM  
\ Client Installation -i silent -DUSER_REQUESTED_RESTART=NO
```

### **Silently Uninstall a PAM Client on Windows**

Use the following procedure to uninstall a PAM Client on Windows without displaying any indication of the process or requiring a reboot.

#### **NOTE**

Starting from 4.1.3, the **CAPAMClient** binary and the **CAPAMClientInstaller** binaries are now 64-bit. The Java version for the PAM client has also been updated to use Java 17.

To use the latest PAM client, do one of the following operations:

- Upgrade your existing PAM client to point to a 4.1.3 (or later) PAM instance.
- Use the installer to install the latest version of the PAM client.

If you choose to upgrade the existing PAM client to version 4.1.3, you cannot use the existing PAM client installer to uninstall this new version.

To uninstall the upgraded 4.1.3 PAM client, follow these steps:

1. Delete the PAM client installation folder.
2. Manually delete the registry key.

If you installed the PAM client as an administrator, delete the registry key in this location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Symantec PAM Client
```

If you installed the PAM client using non-administrative credentials, delete the registry key in the following location:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Symantec PAM Client
```

If you choose to install the 4.1.3 or later PAM client, use the installer to uninstall as needed. You do not need to clean up the installation manually.

**Follow these steps to silently uninstall the PAM 4.0 version of the client:**

#### NOTE

Version 4.0 rebranded the product to Symantec, resulting in a change in the path.

1. Enter the following command:

```
"<Installation location of PAM client>\_Symantec PAM Client_installation\Change  
Symantec PAM Client Installation.exe" -i silent -DUSER_REQUESTED_RESTART=NO
```

**To silently uninstall versions of the client *earlier than PAM 4.0*:** enter the following command:

```
"<Installation location of PAM client>\_CA PAM Client_installation\Change CA PAM Client  
Installation.exe" -i silent -DUSER_REQUESTED_RESTART=NO
```

## Use a Private Content Delivery Network to Distribute the PAM Client Installer

When a user selects the PAM Client download option from the PAM UI logon screen, PAM attempts to retrieve the Client binaries from the Broadcom Public Content Delivery Network (CDN) over the Internet. However, If your site restricts Internet access or if PAM is deployed in a closed network, you must configure a Private CDN to support internal distribution of PAM Client binaries.

### Set Up a Private CDN Repository for PAM Client Binaries

Configure a server that is accessible to all user systems in the PAM environment as the Private CDN repository for the PAM Client binaries.

**Follow these steps:**

1. On the server that is designated as the Private CDN repository, create the following directory structure (exactly as shown) to store the PAM Client binaries:

```
ca-pam/  
+---install/  
    +---linux64    (one or more 64-bit Linux installers)  
    linux86        (one or more 32-bit Linux installers)  
    mac            (one or more macOS X installers)  
    Windows        (one or more Windows installers)
```

For example, you store Linux 32-bit installers in `ca-pam/install/linux86`.

2. From a system with Internet access, download the required PAM Client binaries from the following Broadcom Public CDN addresses each time that you upgrade your PAM environment:

- **Windows:** [https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/win/CAPAMClientInstall\\_Vx.y.z.exe](https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/win/CAPAMClientInstall_Vx.y.z.exe)
- **macOS:** [https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/mac/CAPAMClientInstall\\_Vx.y.z.zip](https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/mac/CAPAMClientInstall_Vx.y.z.zip)
- **UNIX:** [https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/linux64/CAPAMClientInstall\\_Vx.y.z.bin](https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/linux64/CAPAMClientInstall_Vx.y.z.bin)

The `x.y.z` represents the required PAM version number. For major releases, omit the `.z`. For example, to obtain the Windows binary for PAM 4.1.5 use the following address:

[https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/win/CAPAMClientInstall\\_V4.1.5.exe](https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/win/CAPAMClientInstall_V4.1.5.exe)



**NOTE**

If you cannot access the Broadcom public Internet CDN, contact Broadcom Support.

- Copy the downloaded binaries to the appropriate directories on the Private CDN repository. For example, copy Linux 32-bit installers into `ca-pam/install/linux86`

**NOTE**

If a PAM Client connects to a newer PAM server, it automatically upgrades to the new version upon connecting to an upgraded PAM server, using the binaries in the Private CDN.

**Configure PAM to Use the Private CDN**

Once the Private CDN repository is set up, configure PAM to use it by modifying the Client settings.

**Follow these steps:**

- Log in to the PAM UI using an account whose user role has the Global Settings permission (for example, Configuration Manager, Global Setter, or Operational Administrator).
- Go to **Settings, Global Settings, Client Settings**.
- For the Private CDN server in the intranet server (`https://`) field **Distribution Method**, select **Intranet** and enter the fully qualified domain name or IP address of the server of the Private CDN server in the **Intranet Server** field.  
For example, `myserver.example.com/`.  
If the server requires a specific port, add a colon (:) followed by the port number as shown in the following example:  
`myserver.example.com:8080`.
- Select **Save**.

The Private CDN is operational. When a user selects the PAM Client download option from the PAM UI logon screen, PAM retrieves the PAM Client binaries from the Private CDN.

**Ports Not Allowed for the Client**

The PAM Client and the PAM Access Agent cannot use the ports that are listed in this table. TCP and UDP ports are not permitted for incoming or outgoing communication. If you are having trouble connecting to the server through the Client or Agent, verify whether a proxy is configured using an invalid port.

You can see the port assignment in the Client or Agent configuration settings:

- From the Client login page, select the gear icon in the lower-left corner.  
The port setting is on the Proxy tab of the Configuration Settings window.
- For the Agent, select the Options menu, and Proxy.  
The port setting is available for the Manual Proxy Configuration option.

Invalid Ports			
1 tcpmux	53 domain	123 NTP	556 remotefs
7 echo	77 priv-rjs	135 loc-srv /epmap	563 nntp+ssl
9 discard	79 finger	139 netbios	587
11 systat	87 ttylink	143 imap2	601
13 daytime	95 supdup	179 BGP	636 ldap+ssl
15 netstat	101 hostriame	389 ldap	993 ldap+ssl
17 qotd	102 iso-tsap	465 smtp+ssl	995 pop3+ssl
19 chargen	103 gppitnp	512 print / exec	2049 nfs
20 ftp data	104 acr-nema	513 login	3659 apple-sasl / PasswordServer

21 ftp access	109 pop2	514 shell	4045 lockd
22 ssh	110 pop3	515 printer	6000 X11
23 telnet	111 sunrpc	526 tempo	6665 Alternate IRC [Apple addition]
25 smtp	113 auth	530 courier	6666 Alternate IRC [Apple addition]
37 time	115 sftp	531 chat	6667 Standard IRC [Apple addition]
42 name	117 uucp-path	532 netnews	6668 Alternate IRC [Apple addition]
43 nickname	119 nntp	540 uucp	6669 Alternate IRC [Apple addition]

## Deploy the PAM Access Agent for Windows

The PAM Access Agent is a lightweight Windows alternative to the PAM Client.

### PAM Access Agent Advantages

The PAM Access Agent has the following advantages:

- It does not use Java or applets.
- It tunnels through Privileged Access Manager to devices.
- It does not require the configuration of loopback addresses.
- It does not contain a browser, so it does not support Privileged Access Manager administration.
- It has a much smaller installer, storage footprint, and memory requirement.
- It uses Services instead of Access Methods
- It allows viewing of credentials

### PAM Access Agent Feature Support

Service	Network Redirection	Auto-Login	Session Recording	Command Filters	Socket Filters
SSH	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
SSH Transparent Login	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No
RDP	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>
RDP Applications	No	No	No	No	No
RDP Applications with Transparent Login	No	No	No	No	No
Web Portal*	<b>Yes</b>	No	No	No	No
VNC	<b>Yes</b>	No	<b>Yes</b>	No	No
Telnet	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
TN3270 / SSL	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
TN5250 / SSL	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>

\*Web Portal does not support the PAM Browser.

Authentication Method	Support
Local	Yes
LDAP / AD	Yes
RADIUS / TACACS+	Yes
LDAP+RADIUS	Yes
LDAP+RSA	Yes
SAML	No
CA Single Sign-On	No
PIV/CAC / Smart Card	No

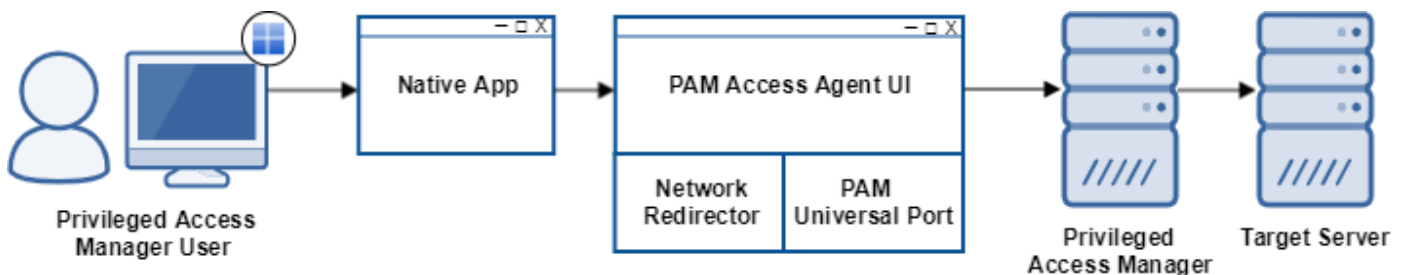
### ***Retrospective Approval Not Supported***

Retrospective Approval (Break Glass) for Password View Requests is a new feature that is not supported yet in the PAM Access Agent.

### **How the Agent Works**

You activate a service in the agent, then network traffic to the target device for that service is redirected and tunneled through PAM. The new agent Universal Port (UP) for Windows provides the service connection capability into PAM. For each activated service and target device, the UP generates the ephemeral port number on which the UP is listening for connections. Client applications (such as PuTTY) work seamlessly using the same public IP address and port they typically use for that connection. Once the service is deactivated, the client application is available for use with targets that are not protected by PAM.

**Figure 16: PAM Access Agent Architecture**



### **Download the Agent Software**

Download the PAM Access Agent for Windows from the browser-based UI login page. To install the PAM Access Agent for Windows, the user needs the same user rights or permissions as any other application that you install.

### **Follow these steps:**

1. From your client workstation, open a browser and navigate to the URL of a PAM server using *one* of the following formats:

`https://server_ip_address/`

`https://fqdn_of_server`

*server\_ip\_address* or *fqdn\_of\_server* is the system where you installed the PAM server.

Examples:

- <https://102.200.11.222/> (IPv4), [https://\[fd6d:8d64:af0c:1:0:242:22:233\]](https://[fd6d:8d64:af0c:1:0:242:22:233]) (IPv6)
  - <https://capam.forwardinc.com>
2. When the PAM UI login screen opens, select the arrow next to **Symantec PAM Agent**. Context-sensitive controls open as highlighted in the following screen capture:

The screenshot shows the Symantec Privileged Access Manager login interface. At the top, there is a logo and the title 'Symantec Privileged Access Manager'. Below this, there are input fields for 'User:' and 'Password:', both marked with an asterisk. An 'Authentication Type' dropdown menu is set to 'Local'. A blue 'Login' button is positioned below these fields. Further down, there is a section for 'Symantec PAM Client' and 'Symantec PAM Agent'. The 'Symantec PAM Agent' section is highlighted with an orange border and contains a 'Platform' dropdown menu set to 'Windows' and a blue 'Download' button.

3. Save the installer file locally to your workstation.

### Install the Agent

#### **NOTE**

**Installation Requirements:** Only 64-bit Windows 10 is supported in version 3.4.

After you download the installer file, run the agent installer. You need local administrator rights to install the agent, but not to run it. Follow the installation wizard, noting the following instructions:

- **License Agreement:** To accept the license agreement, scroll through the license text to the bottom of the panel.
- **Destination Folder:** Accept the default or select **Change** to find a folder.

#### **NOTE**

The PAM Access Agent does not support installation in directories whose names include Japanese characters. If you install the PAM Access Agent on a Japanese-language computer, enter a folder with no Japanese characters.

- When the installation is complete, a **Launch PAM Agent** checkbox appears. Select it and then Finish to close the installation and log in with the agent.

## Open the Agent

As a user, all you need is the Fully Qualified Domain Name (FQDN) or IP address of your Privileged Access Manager instance, and your user name and password.

### Follow these steps:

1. Open the PAM Access Agent.
2. Select the **Options** menu to set the log level, certificates, and proxy, if necessary. See [Optional Settings](#) for details.
3. In the **PAM Server/IP** field, enter the IP address or the assigned fully qualified domain name of the PAM Server or cluster VIP.
4. Select **Connect**.
5. You may receive a **Verify Certificate** window before the login screen appears. If you approve of the certificate, select the **Import this certificate permanently** checkbox. Select **Continue**.  
Once it is trusted, you should not see the certificate warning any more.
6. If an agent update is available, a dialog appears. If you select **Yes**, an installation dialog appears. Select **Yes** to upgrade the agent. Upgrading the agent is not mandatory.
7. When the login screen appears, enter the **User Name** and **Password**.
8. Select the **Authentication Type**.
9. Select **Login**.  
The Available Services tab appears, listing devices that you have permission to access. A Filter panel appears above the list allowing you to reduce the number of listed services.

## Optional Settings

An **Options** menu allows you to configure optional settings that might be required for your particular environment:

### Logging

Use this option to select the amount of application messaging:

- **Info:** Default setting, including error, and informational messages; medium amount of information
- **Debug:** All messages, including warnings, errors, informational messages; most information
- **Error:** Only log errors; least information

### Certificates

The Certificate Authorities (CA) window lists CAs that are trusted by the PAM Access Agent. You can perform the following actions:

- **Import:** Use this button to import your own certificates.
- **Export:** Use this button to export a certificate to a location on your local computer.
- **Remove:** Use this button to remove any certificates that you do not want.

### Proxy

Indicate whether the PAM Access Agent is connecting to the PAM server through a proxy server. Select one of the following options for your deployment:

- **No Proxy** (default): The agent connects directly to the PAM Server.
- **Auto-detect proxy settings for this network:** For a network-managed proxy. The agent executes the script that is retrieved from `http://wpad/wpad.dat` to determine which proxy server to use.
- **Use system proxy settings:** For workstation OS-managed proxy. On Windows, you can configure it using the `netsh winhttp set proxy` command.
- **Manual Proxy Configuration:** For a custom target device as the proxy
  - Enter the **Host** and **Port** of the Proxy server.

The agent cannot use most well-known ports. See [Ports Not Allowed for the Client](#) for the full list.

- Enter IP addresses to **Bypass**, such as 127.0.0.1 or 192.168.\* (for IPv4), or fe80:250:56ff:1111:2222:3333:\* (for IPv6)

To enter more than one address, separate each address with a comma, such as 127.0.0.1, 192.168.\*

- **Automatic proxy configuration URL:** for a web server-supplied proxy. The agent executes the Proxy Auto-Configuration (PAC) script that is retrieved from the URL to determine which proxy server to use.

### Timeouts

Specify timeout values for receiving a response to requests to the PAM Server:

- **Receive Timeout:** Specifies the timeout (in seconds) for receiving a response to requests to the PAM Server. The default value is 5 seconds.
- **3rd Party Authentication Timeout:** Specifies the timeout (in seconds) for receiving a response to requests to the PAM Server when third-party authentication (for example, Radius, RSA, and so on) is required. This value is used instead of **Receive Timeout** for such requests because third-party authentication generally takes longer. The default value is 90 seconds.

### Activate a Service and Connect to a Device

The PAM Access Agent uses Services instead of Access Methods. The agent ignores the **Client Application** field in a TCP/UDP Service configuration. The Agent does not open the client application for you.

The PAM Access Agent displays three tabs: Available Services, Activated Services, and Credentials.

**Available Services** lists devices that you have permission to access. You can select the column headings to sort the rows in ascending order by that field. Select a second time to sort in descending order.

- **Device Name:** The device name
- **Address:** The IP address of the device
- **Port** to connect to the service
- **Operating System** of the Device
- **Service:** The name of the service

Activated **Services** displays any service which is activated for use by a local application.

- **Device Name:** The device name
- **Address:** The IP address of the device
- **Port** to connect to the service
- **Operating System** of the Device
- **Service:** The name of the service
- **Credential:** The credential that you have selected to use with this service.

The **Credentials** tab lists the credentials available for you to view. There can be multiple credential rows for each device.

- **Account Name:** Target account for connecting to the listed device, and password viewing, if applicable.
- **Application Name:** Target application for connecting to the listed device, and password viewing, if applicable.
- **Device Name:** The device name
- **Address:** The IP address of the device
- **Status:** Dual-authentication status, such as Pending or Approved
- **Action:** Select **View Password** to view the password for this account.

### To connect to a device, follow these steps:

1. On the Available Services tab, double-click the Device row to activate the device connection. You can also enter or right-click to activate a service.
2. If there are multiple available credentials, the **Select Credential** window appears.

3. Select the **Credential** to use, and then **OK**.
4. Open the application that you use to connect to the device.
5. Enter the FQDN or IP Address of the device and port in the native application.  
The native application connects to the device.

**NOTE**

You might receive a security alert the first time that you try to connect using a native application with the agent activated. For example, PuTTY expects to connect to the target device, but the agent is redirecting traffic to Privileged Access Manager, where PuTTY obtains the key fingerprint. Therefore, it warns of a "potential security breach."

6. At the login prompt, hit Enter. The account name is automatically sent.  
If credentials are configured, they are also automatically sent.
7. When you are done using the PAM-managed device, right-click its row on the Activated Services tab and select **Deactivate Service**.
8. When you are done, **Log Out** from the PAM Access Agent.

**NOTE**

If a Service or Credential has become available since you logged on, select the **Refresh** button on the PAM Access Agent to display it.

**View Passwords**

Use the **Credentials** tab to select a credential to view. There can be multiple credential rows for each device.

Select **View Password** to view the password for an account.

**Silent Installation**

To install the PAM Access Agent in silent mode from a Command Prompt (as Administrator), use the following command:

```
CAPAMAgentInstall.exe /s /v"/qn"
```

To change the default installation directory, use this command:

```
CAPAMAgentInstall.exe /s /v"/qn INSTALLDIR=path_to_install_directory"
```

**Troubleshooting*****Network Error***

If you receive a "Network error" such as "Permission denied" or "Connection refused", you probably have a network redirection failure. You can resolve this error in several different ways:

- Run `CAPAMAgent.exe` as Administrator from a Command Prompt.
- Run the `CAPAMAgentCleanup` utility:
  - a. Log out from PAM Access Agent.
  - b. Run `CAPAMAgentCleanup.exe` (found in the installation folder) as Administrator from a Command Prompt.  
Any network redirectors are removed.

***DNS Resolution***

A Target Server Address can be defined in Privileged Access Manager using a DNS host name rather than an IP address. If the PAM Access Agent does not have access to an appropriate DNS server, it cannot resolve the host name.

***Language Mismatch***

PAM Access Agent does not support using a different language than the locale of the PAM Server. If the server is set to Japanese, and the agent computer is English, server communication tries to render in Japanese, but it shows non-Kanji

symbols. The agent user interface would be English, but dynamically generated drop-downs, such as password view reasons, and error messages, would be symbols. If both server and agent are the same language, whether English or Japanese, this problem does not occur.

### **Uninstall the Agent**

Use one of the following methods to remove the agent:

- Remove the PAM Access Agent from the **Windows Control Panel, Programs and Features**.
- Open the PAM Access Agent installer and select the **Remove** option.

## **How to Set Up a Cluster**

To protect your deployment from performance issues or failure, configure a *cluster*. A typical cluster consists of one or more sites (typically one per data center), each containing multiple PAM server instances (*nodes*). Server data is kept in sync between nodes in primary site or in a single site cluster using MySQL 8 Group Replication. Server data is kept in sync between the primary site and nodes at secondary sites using traditional MySQL 8 Replication.

Each site is then addressed by a single *virtual IP address (VIP)* that distributes requests between member nodes using [internal \(PAM software-based\)](#) or [external load-balancing](#). Each site in the cluster therefore operates as a single virtual system, providing support for the following benefits and capabilities to your PAM deployment:

- Improved throughput
- Expanded capacity
- Redundancy
- Disaster recovery

This article contains the following topics:

- [Single-and Multiple-Site Clusters](#)
- [Properties Of Single-Site Clusters and Primary Sites In Multi-Site Clusters](#)
- [Differences Between Primary and Secondary Sites and Their Members In a Multi-Site Cluster](#)
- [Internal and External Load-Balancing](#)

### **Single-and Multiple-Site Clusters**

Configure a *single-site cluster* or *multi-site cluster* using the following guidelines to help determine which best suits your requirements:

- **Separation of administrative and access tasks:** To designate specific PAM nodes to handle global administrative functions (such as policy maintenance and credential rotation) and others to handle user requests for access to privileged devices, configure a [multi-site cluster](#). Address all administrative requests to the VIP of the primary site and all access requests to the VIPs of secondary sites.
- **Geographical distribution of data centers:** If all your PAM nodes are deployed at a single geographical location and you do not need to separate them for administrative and access tasks, you only require a [single-site cluster](#). If your PAM servers are deployed over multiple geographically dispersed locations, configure a [multi-site cluster](#).

### **Single-Site Clusters**

If all your PAM infrastructure is deployed at a single geographical location and you do not require separate administrative and access tasks between nodes, you only require a *single-site cluster*. PAM replicates data across all the nodes so that they operate as a single virtual system addressed by a single VIP.

#### **NOTE**

Whenever you add another site to a single-site cluster, the first site you configured becomes the *primary site* for the new multi-site cluster. Once created, any site in the multi-site cluster can be promoted to become the primary site. For more information, see [Site Promotion Using Replication Analysis](#).



## Multi-Site Clusters

If your PAM environment is deployed over multiple geographically dispersed locations or you want to designate specific nodes to handle administrative activities (recommended), configure a *multi-site cluster*. The primary site in a multisite cluster must contain an odd number of members. Multi-site clusters have one *primary* site and one or more *secondary* sites. Each site is addressed by its own VIP.

- **Primary site** members are co-located and are typically designated for administrative activities (policy maintenance, credential rotation). If user requests for access to privileged devices must also be handled at the same data center, create and designate a secondary site at the same location for that purpose. Data that is saved on one member of the primary site is synchronously replicated across all primary site members. Only one primary site exists within a cluster at any time.

### NOTE

The primary site in a multi-site cluster behaves the same as a single-site cluster with the same properties. primary sites and single-site clusters both use group replication to keep themselves in sync.

- **Secondary site** are typically designated for access activities, that is, handling user requests for access to devices. Asynchronous replication is performed from the primary site to secondary sites. Replication allows secondary site members to recover gracefully and continue operating should a network issue exist between the sites, like a brown-out or DC outage.

### NOTE

A secondary site can also be promoted to primary site status, providing a warm backup if the primary site goes down. For more information, see [Cluster Synchronization, Promotion, and Recovery](#).

## Properties Of Single-Site Clusters and Primary Sites In Multi-Site Clusters

Single-site clusters and primary sites in multi-site clusters have the following properties:

- **Colocation:** All members of a single-site cluster should be colocated in the same data center. Group replication is best supported in geographical proximity. If you have remote data centers, create a multi-site cluster where each remote data center is a secondary site.
- **Primary leader:** The first cluster member that is listed in the primary site is designated as the *primary leader* and is the data synchronization source for all cluster members.
- **Cluster size:** A primary site is limited to nine member nodes. We recommend three and a maximum of five members. (See **Quorum**.) The more members that you add, the more communication work the cluster has to do. The total number of members in all sites is limited to 1,000.

### NOTE

If the entire cluster has only two members, do not put both members in the primary site. Instead, create a 1 x 1 configuration (one member at the primary site and one member at a secondary site). For more information, see [Primary Site Fault Tolerance](#).

- **Quorum:** In MySQL Group Replication, a "quorum" is the number of members that are required to make decisions for the cluster, such as whether a member has failed. The quorum is the majority of cluster members, or in this case the primary Site. For this reason, we recommend an odd number of members, such as 3 (whose quorum is 2), or 5 (whose quorum is 3). However, we do support fewer members.
- **Data replication:** Changes to administrative and Credential Management data can be made through any member and can propagate to the other members. When starting the cluster, the database from the first member is replicated to the other members, overwriting their data. Member-specific information, such as logs and some configuration data are not replicated.
- **Disaster recovery:** Add a secondary site (creating a multi-site cluster) to a single-location deployment to provide a warm backup for disaster recovery.

## Differences Between Primary and Secondary Sites and Their Members In a Multi-Site Cluster

Primary and secondary sites and their members in a multi-site cluster have the following important differences:

- There can only be one primary site, which is the source of data for all secondary sites.

#### **IMPORTANT**

If the primary site fails, you must *manually* promote a secondary site to be the primary site to restore cluster operation.

- Secondary site members are typically intended to support end-user access rather than global administrative functions, which are typically handled on the primary site. Some local administrative functions are available on secondary site members, including: managing sessions, logs, and recordings; managing password approvals, viewing credentials, and disaster recovery; some diagnostics; network, and security.
- Secondary sites, with few exceptions, do not support REST API or CLI operations. (The specific CLI command documentation mentions this, as in [checkInAccountPassword](#).) Use the VIP of the primary site for REST API and CLI commands.
- The best practice is to have each member of a particular secondary site in the same data center.
- Each secondary site has a leader which receives updates from the primary site. The secondary leader then replicates the data to the other site members and relays updates from secondary members to the primary site. This topology minimizes WAN traffic between the sites.
- If the secondary leader goes offline, the other site members communicate directly with the primary site.
- Secondary members can “self-heal” after being disconnected. See [Cluster Synchronization, Promotion, and Recovery](#) for details.
- Members can be added or removed from secondary sites without stopping the cluster. This process requires a VIP for the site you are subscribing to.
- Multi-site clustering uses MySQL 8 traditional asynchronous replication to communicate between primary and secondary sites. Almost all data changes start with data on a primary site node. When replication starts with data on a secondary site node, it first is replicated to the primary leader and the data is distributed normally from there.

### **Internal and External Load-Balancing**

PAM clustering supports internal and external load-balancing solutions which you configure at the *site level*. That is, multi-site clusters support individual sites that are configured with different load-balancing solutions. For example, in a three site cluster, the primary site and one secondary site can be configured to use an External Load Balancer. The third site can be configured to use PAM Floating IP load-balancing.

Specify the load-balancing solution for each site in your cluster by specifying one of the following **VIP Address Type** settings:

- **Floating IP:** (Default) Use the internal PAM software-based load-balancing solution in which requests addressed to the VIP are handled by the *site leader* (the first node added to the site) which redirects them to the least-loaded site member. If the site leader is down, the next node is automatically promoted to be the site leader, and so on, until the site leader is back online (This was the only load-balancing option before release 4.1).
- **External Load Balancer:** Use an external load-balancing solution to handle requests that are addressed to the VIP and redirect them to one of the cluster site members based on the external load balancer algorithm.

#### **NOTE**

For important guidelines for configuring external load balancers, see [External Load Balancer Configuration Guidelines](#)

### **Next Steps**

- [Cluster Deployment Requirements and Guidelines](#)
- [Configure a Cluster](#)
- [Cluster Synchronization, Promotion, and Recovery](#)
- [Configure Load Balancers to Determine the Availability of Cluster Nodes](#)

## **Cluster Deployment Requirements and Guidelines**

Before you configure a cluster, verify that your environment meets the following requirements:

## Network Requirements

Your environment must satisfy the following network requirements:

- **High Network Availability:** Clustering in the primary site uses synchronous SQL replication, which requires a high network uptime to avoid network loss. If the network is down, cluster members eventually time out and they are deactivated. A deactivated cluster member can cause synchronization problems.
- **DNS:** Note the following best practices:
  - Primary DNS uptime to avoid latency in the product UI and its subsystems. Maintain the primary DNS server to avoid failover to a secondary DNS.
  - Unique appliance host names: If host names are the same, logging, and other metrics are negatively impacted.
  - Register host names and IP addresses in the DNS for forward and reverse look-ups.
- **Internet Control Message Protocol (ICMP):** The internal active-active control uses ICMP ping to monitor network conditions.

### TIP

ICMP connectivity and LAN gateway require high uptime to reduce the cost of network loss.

Failed ICMP triggers a cluster member to enter isolation mode, implying that a communication failure between members is in progress. Restored ICMP during an isolated mode triggers an automated merge recovery. A merge recovery requires service download proportional to DB size and cluster size. The cluster automatically stops, then one database is copied and restored on all other appliances, and then the cluster restarts.

- **Network Time Protocol (NTP):** The product is pre-configured with default NTP servers, but these require internet access. If the cluster is not routed to the internet, use local LAN NTP servers to ensure that cluster members are set to the same time.
  - Configure the NTP in the GUI by selecting **Configuration, Date/Time**.
  - NTP server connectivity is checked during startup. If the times between appliances differ by 3 seconds or more, the cluster does not start. After a cluster starts, NTP server connectivity is not monitored so external monitoring is required.
- **TCP:** Do not permit TCP blocking, throttling, or traffic shaping on any part of the LAN, VLAN, or WAN for the following ports and protocols:
  - **Clustered appliance:** Within a site, these ports are required: TCP/443, 8443 (HTTPS); TCP/3307, 13307 (MySQL); TCP/5900 (Hazelcast). Between sites, only 443, 8443, and 3307 are required. For external user access, only 443 is required. (For a standalone appliance, only TCP/443 is necessary.)

### NOTE

TCP ports 3307 and 13307 must be set **Open**, not **Filtered**.

- **Socket Filter Agent (SFA) clients:** TCP/8550 (plus protocol-specific ports for RDP, SSH, and other access methods)
  - **A2A clients:** TCP/28888
  - **Windows Proxy:** TCP/27077
- See [IP Addresses and Ports for Network Connectivity](#) for more information.
- **Subnet:** The VIP and every member of a particular site must be in the same subnet.

## PAM Server Requirements

Before you implement a cluster, each member must have at least the following items configured:

- **Licensing:** Other than the Hardware ID, all cluster members need the same settings. See the [Licensing](#) configuration page for more information.
- **Network:** Some settings differ for each member. Ensure that the **Hostname** is different for each member. See the [Network configuration](#) page for more information.
- **Date/Time:** Ensure that the time server is specified correctly. See the [Date and Time configuration](#) page for more information.
- **Clustering:** Enter the same Shared Key on each member and save it there by selecting **Save Locally**. Once the cluster starts, the remaining cluster configuration is replicated to all members.
- **Use only IPv4 or IPv6 addresses.** Use only IPv4 or IPv6 addresses for addressing appliances in a cluster.
- **Ensure that all cluster members use the same software release.** Verify that each cluster member is running the same release of the product software. If not all members are at the same release (patch) version, upgrade all members to the latest release in the cluster.
- **All members of a Primary or Secondary site must be on the same platform.** A site can be on one platform: AWS, VMware, Azure, or hardware appliance
- **FIPS:** If any member of cluster is FIPS enabled, then all members must be FIPS enabled.

#### NOTE

You cannot change these values while the cluster is running.

### **External Load Balancer Configuration Requirements and Guidelines**

When using external load balancing, consider the following information when configuring the load balancers:

- All PAM servers in the cluster must be running PAM 4.1 or later.
- Deploy and configure a Layer 4 network load balancer for each site in the cluster that is configured to use external load balancing.
- Configure the load balancer to listen to port 443 on the VIP address configured in the PAM site definition.

#### NOTE

SSL connections do not terminate at the load balancer.

- Configure the load balancer to distribute incoming traffic to the local IP addresses of the members of the site.
- Enable Session Affinity and, if possible, configure the timeout value to be slightly longer than the login timeout value of the cluster members.
- Enable X-Forwarded-For header for A2A request servers (if applicable).

#### NOTE

If your load balancer does not support the X-Forwarded-For header, the following functionality may not work: auto-registration of request servers, auto-registration of Windows Proxy agents navigate navigate to work, and the creation of utility groups.

### **WAN Link Cluster Requirements**

You can use a WAN link between sites in a size cluster.

To use a WAN link, confirm the following requirements:

- Use only a public IPv4 address for the VIP (Virtual Management IP), as the cluster members are not on the same subnet.
- Be mindful that network packet loss is not excessive.
- Confirm that your NTP servers are running properly then turn on the cluster. Look the Date/Time page, NTP Status panel (`aactrl` output) to see that the following conditions are met:
  - "remote" column: At least one primary NTP server (denoted with a \*) is available
  - "offset" column: The absolute value of this field must be less than 3000
  - "when" column: This field must be less than 5 times the value in the poll column (the poll frequency)

Look for a summary message in the session logs, and then immediately address the NTP servers. An example log entry with an unacceptable value is shown:

```
NTP problem on member 10.0.0.21. NTP Server: *6.175.209.17: Offset: 1.1.51 (should be
< 3000), Poll: 64, When: undefined (when should be < poll *5)
```

- Assign a unique host name to each cluster member.

### **FIPS Certificate Requirements**

If you configure FIPS on your cluster, you must enable it before setting up the cluster. You must enable FIPS on each member of the cluster, including secondary sites. For more information about FIPS, see [Configure Enhanced Encryption for Stored Credentials](#).

### **AWS AMI Cluster Requirements**

To use AWS AMI instances in your cluster, set up your AWS environment correctly.

#### **Follow these steps:**

1. Create an AWS virtual private cloud (VPC) with at least one public subnet in which to locate your cluster. Assign an AWS Security Group that permits intra-subnet communication, inbound and outbound traffic through ports 3307, and 13307 (for MySQL).

#### **NOTE**

Ports 3307 and 13307 must be set **Open**, *not Filtered*

2. Configure the members of your AWS cluster and assign them to the VPC you created. Note the local subnet address for each.
3. Create an elastic IP address (EIP) for each member of your cluster and assign it to that member. Note which EIP is assigned to which instance.
4. Create an extra EIP to serve as the cluster VIP address, but do not assign this EIP to any instance.

#### **NOTE**

AWS Elastic Load Balancing (ELB) is incompatible with PAM internal (Floating VIP) load-balancing. However, you can configure an AWS ELB as the load-balancer for a site that is configured to use external load balancing.

To set up clusters on other AWS sites, AWS connections have to be configured in Privileged Access Manager. To configure the AWS connections, see [AWS Coordination](#).

### **Azure Cluster Requirements**

To build a cluster of Azure instances, follow these steps in your Azure environment. First set up your individual instances in Azure. See [Configure an Azure Connection](#). We recommend creating a separate virtual network for each Primary and Secondary site to avoid DHCP conflicts that might occur while the cluster is off.

Privileged Access Manager clustering uses Azure APIs which requires Azure credentials. In particular, the Azure VIP assignment requires Azure credentials. When you start the cluster, Privileged Access Manager creates an IP configuration for the VIP in the primary node Network Interface (NIC). If the primary node is unavailable, Privileged Access Manager deletes the VIP configuration from the primary node and creates it in the NIC of the next node.

#### **NOTE**

If you want to use an IPv6 cluster for PAM instances deployed in Azure, you cannot use a Floating IP as the IPv6 VIP address. You must use an external load balancer while configuring the IPv6 VIP address.

#### **Create a VIP for Each Azure Region**

1. On the Azure Portal, select **All Services**, and enter a "Public IP address."

2. Select **+Add** to create a public IP address.
  3. Enter a **Name**.
  4. Select **Static** for **IP Address Assignment**.
  5. For **Resource Group**, select **Use Existing** and select the Resource Group for your PAM instances.
  6. Select **Create**.
- This public IP address of your VIP is used in the PAM cluster configuration as the "VIP NAT Address."

### Create A Private IP Address for Your VIP

1. On the Azure Portal, select **Virtual Networks** from the left menu.
2. Select the Virtual Network for your PAM instance.
3. Select **Networking**.
4. Select your **Network Interface**.
5. Select **IP configurations** from the left menu.
6. Select **Add**.
7. Add a **Static IP Address** to the same subnet as the PAM server. This is the Private IP address for your VIP.
8. Associate the Public IP address with the Private IP address that you just added.
9. Record the Private IP address to use as the "VIP Address" in the PAM cluster configuration

## Configure a Cluster

Configure a cluster from the **Clustering** pane in the PAM UI. Configure each member in the cluster individually then activate the cluster by turning on synchronization. The exception to this rule is the configuration of third-party authentication, which is replicated.

### Follow these steps:

1. Log in to the UI on a PAM server that will be a member of the primary site.
2. Navigate to **Configuration, Clustering**.  
The **Clustering** page appears with the **Local Settings** tab selected.
3. Do the following steps on the **Local Settings** tab:
  - a. Use the controls in the **Shared Key** section to specify a 32-bit shared key for all members of all sites in the cluster to secure communications between them. (Do not use the same Specify shared key on separate clusters.)  
Use one of the following methods to generate the initial key:
    - Enter a **Passphrase** and select the **Generate Key** button. The **Key** field is populated with the generated value.
    - Use a third-party tool or the following OpenSSL command in Linux or Cygwin: `openssl rand -hex 16`. Enter the returned value in the **Key** field. (Required if operating in **FIPS Mode**, when the **Generate Key** button is disabled.)

Once the shared key is generated, use it to manually populate the **Key** field on all other instances in the cluster.
  - b. Specify network interfaces to use for IPv4 and IPv6 (or both, if applicable) communication between clustered appliances using the dropdown menus in the **Interfaces** section:

#### NOTE

To verify which network interfaces are configured with IPv4, IPv6, or both addresses, refer to the **Network Interfaces** section on the **Configuration, Network, Network Settings** panel.

#### NOTE

If AWS or Azure is being used, both **Interface** controls are dimmed and unavailable.

- **IPv4 Interface:** Select a network interface with an IPv4 address.
- **IPv6 Interface:** Select a network interface with an IPv6 address.

#### NOTE

Specify the same interface values on every member of the cluster.

- c. Select **Save Config Locally**. The same interface must be used by all the clustered members.
4. Select the **Global Settings** tab and do the following steps:
  - a. Under **Multi-Site**, determine the behavior of the secondary site when the primary site is unavailable. To change the behavior globally, first turn off the cluster. The options for the secondary site are:
    - **Operationally Safe**
      - Users can view passwords from the local PAM database.
      - Users can continue to access devices and can create sessions to devices.
      - All workflow functions are disabled. These functions are check-in/check-out, dual authorization, credential rotation, Service Desk integration, and reason to view credentials.
    - **Security Safe**
      - Users cannot create sessions to devices that are configured for auto-login using Credential Manager.
      - Users cannot view passwords.

Workflow functions are not available when the primary site is down.

- b. On Secondary sites, the **Disaster Recovery** tab defines the behavior of an *individual* secondary site member in case the primary site fails. For a secondary member to behave in Operationally Safe mode, keep the **Run Secondary Site in Operationally Safe Mode** checkbox selected. To run in Security Safe mode, clear this checkbox.
- c. Use the buttons under **Sites** on the **Global Settings** tab to add primary and secondary sites, add members to those sites, and administer them. Add a site manually or load the configuration from an existing cluster member. See [Add a Cluster Site](#) for instructions.
- d. To receive email notifications of the following types of cluster events, select the **Notification** tab then set the **Enable Email Notifications** option:
  - **Group Replication Quorum Failure**: Notifies the configured administrator when a MySQL group replication quorum failure has occurred.
  - **Group Replication Quorum Recovery**: Notifies the configured administrator when a MySQL group replication quorum failure has occurred and that PAM is going to reboot each member of the cluster.
  - **Member - Out of Sync**: Notifies the configured administrator when a cluster member has now been marked out of sync.
  - **Member - Timeout**: Notifies the configured administrator when a cluster member has timed out.
  - **Member - In Sync**: Notifies the configured administrator when a cluster member that was previously out of sync is now in sync again.

#### NOTE

Email notifications are sent to the **Admin Email** that is set at **Configuration, Monitor**. This setting is not replicated, so each primary member needs the email set separately. Each member should have the same monitor settings.

### Start the Cluster

When your cluster is configured, use this procedure to start it.

#### Follow these steps:

1. Open the PAM UI on any node in the primary site and login as an administrator with configuration privileges (for example, "config" or "super").
2. Navigate to **Configuration, Clustering**, and select the **Global Settings** tab.
3. Select the **Turn Cluster On** button at the bottom of the page.

### Stop the Cluster

Use this procedure to stop a cluster.



**Follow these steps:**

1. Open the PAM UI of any node in the primary site using its IP address or FQDN (do *not* use the site VIP address) and log in as an administrator with configuration privileges (for example, "config" or "super").
2. Navigate to **Configuration, Clustering**, and select the **Status** tab.
3. Select **Turn Cluster Off** button at the bottom of the page. Wait until a notification indicates that synchronization is off

**Next Steps**

- [Add a Cluster Site](#)
- [Add a Cluster Member](#)

**Add Sites to Your Cluster**

This content describes how to add sites to an [existing PAM cluster](#).

**IMPORTANT**

Each site member that you add must be configured with the same **Shared Key** and **Interface** values, as described in [Configure a Cluster](#).

**NOTE****IPv6 Addressing Prerequisites**

If you are configuring your cluster to use IPv6 addressing, verify that the following prerequisites are met:

- Verify that the PAM environment is IPv6-enabled and that at least one network interface with an IPv6 address is configured. For more information, see [Configure Network Settings](#).
- Verify that the **IPv6 Interface** menu on the **Configuration, Clustering** panel **Local Settings** tab specifies an interface with an IPv6 address

**Guidelines for migrating an existing IPv4 cluster to IPv6:**

- All the nodes in the cluster must be IPv6 enabled.
- Primary and Secondary node sites within a cluster must all use either IPv4 or IPv6 addresses. You cannot mix site address types.
- To support components that *are only addressable using IPv4* (such as A2A clients), configure at least one IPv4 VIP address for the cluster.

**Add a Cluster Site**

Follow this procedure to add a site to your cluster.

**To add a cluster site, follow these steps:**

1. Log in to the PAM UI on a primary site member.
2. Navigate to shared **Configuration, Clustering** page.
3. On the **Global Settings** tab, select the **Add** button.  
The **Add Cluster Site** page opens.

**NOTE**

The first site that you add is designated as the Primary Site. The first cluster member provides data for the initial sync. If that member fails, the next cluster member takes the primary role.

4. Enter a **Site Name**, which can be anything that helps you logically group the site members. For example: West coast, NYC, EMEA, or Primary.
5. Select the appropriate **PAM Appliance/Instance Platform**: one of **On-premises**, **AWS**, or **Azure**.  
For AWS or Azure instances, a drop-down list of your provisions appears:



- If you specified **AWS**, select the appropriate entry from the **AWS Provision** drop-down list that appears. The list includes only regions that you have configured in AWS connections. If you are using a cluster in AWS, see [AWS AMI Cluster Requirements](#).
- If you specified **Azure**, select the appropriate entry from the **Azure Provision** drop-down list that appears. The list includes only regions that you have configured in Azure connections. If you are using a cluster in Azure, see [Azure Cluster Requirements](#).

**NOTE**

If you want to use an IPv6 cluster for PAM instances deployed in Azure, you cannot use a Floating IP as the IPv6 VIP address. You must use an external load balancer while configuring the IPv6 VIP address.

6. Complete the following **Load Balancing** settings:

- **VIP Address Type:** Specify the load-balancing solution for each site in your cluster by specifying one of the following **VIP Address Type** setting options. For **important** guidelines for configuring external load balancers, see the [External Load Balancer Configuration Guidelines](#) section of the [Cluster Deployment Requirements and Guidelines](#) topic. When accessing a cluster, use the VIP address, NOT the Member address.
  - **Floating IP:** (Default) Use the internal PAM software-based load-balancing solution that uses the site leader (the first node that was added to the site) to handle requests that are addressed to the VIP. The site leader redirects these requests to the least-loaded node. If the site leader is down, the next node is automatically promoted to be the site leader, and so on, until the site leader is back online.
  - **External Load Balancer:** Use an external load-balancing solution to handle requests that are addressed to the VIP and redirect them to one of the cluster site members based on the external load balancer algorithm.
- **IPv4 and IPv6 VIP settings:** To configure VIPs to access the cluster using IPv4, IPv6, or both addressing, populate the following fields:

**NOTE**

We recommend always using a VIP. If a site has only one member, the VIP is not required. However, if the site has more members, or if you plan to add members later, then a VIP is required.

- **IPv4 VIP Address:** Enter a virtual address (VIP) to use to access the cluster using IPv4 addressing. Through a firewall, or for AWS, enter a mapped address in the form [local\_address or aws\_vpc\_ip], [NAT or aws\_eip]. For examples, see the following chart.

Local or AWS VPC IP	NAT or AWS EIP
10.0.0.59,	107.23.143.123
10.0.0.59,	capam1.example.com
10.0.0.59,	capam1.example.com:4443

**WARNING**

The cluster VIP and its members must be in the same subnet.

The cluster is always available for all users through this virtual IP address. The primary appliance uses its defined VIP, and redirects user requests to the least-loaded member of the cluster.

- **IPv4 VIP NAT Address:** If you are using NAT for the IPv4 VIP, add its IP address here.
- **IPv4 VIP Host Name:** Enter a DNS machine name that is used to access the cluster using an IPv4 VIP. Users adding a DNS name to their VIP settings should enable this configuration.
- **IPv6 VIP Address:** Enter a virtual address (VIP) to use to access the cluster using IPv6 addressing. Through a firewall, or for AWS, enter a mapped address in the form [local\_address or aws\_vpc\_ip], [NAT or aws\_eip]. For examples, see the following chart.

Local or AWS VPC IP	NAT or AWS EIP
fd6d:8d64:af0c:1:250:56ff: feb1:7a4a	2600:1f18:4c6e:9f00:56e1:a630:3a41:1b65
fd6d:8d64:af0c:1:250:56ff: feb1:7a4a	capam1.example.com

fd6d:8d64:af0c:1:250:56ff: feb1:7a4a

capam1.example.com:443

**WARNING**

The Cluster VIP and its members must be in the same subnet.

The cluster is always available for all users through this virtual IP address. The primary appliance uses its defined VIP, and redirects user requests to the least-loaded member of the cluster.

**NOTE**

We recommend always using a VIP. If a site has only one member, the VIP is not required. However, if the site has more members, or if you plan to add members later, then a VIP is required.

- **IPv6 VIP NAT Address:** If you are using NAT for the IPv6 VIP, add its IPv6 address here.
  - **IPv6 VIP Host Name:** Enter a DNS machine name that is used to access the cluster using an IPv6 VIP. Users adding a DNS name to their VIP settings should enable this configuration. Use this field to enter a Fully Qualified Domain Name and, if desired, a port number. Ports are only supported when entered with the FQDN. To enter a port number, enter the <FQDN>:<port number>.
  - **Internal Cluster Communication:** Specify whether to use IPv4 or IPv6 addressing for communication between cluster members:
    - **Use IPv4 VIP addressing requirements** (the default):
    - **Use IPv6 VIP:**
7. When [Cluster Tuning](#) mode is on, four **Database Replication** settings are available. Change these settings only if directed to do so by Broadcom Support:
- **Connection Timeout (seconds):** Set the time for a primary site member to wait to connect to a peer primary site database before failing. Timeouts can lead to deactivation of the member database.
  - **Socket Timeout (seconds):** Set the time for a primary site member to wait for a response from a peer primary site database before failing. Timeouts can lead to deactivation of the member database.
  - **Download Database From Secondary Site Leader:** Set this option (the default) To efficiently distribute the database, the initial startup mimics the replication pattern of sending data to the secondary site leaders. The secondary site members get their initial database from their site leader, using faster LAN speeds. This can speed up cluster startup, depending on your cluster size and WAN speeds. It also allows secondary sites to be available once their leader is ready, before the other site members are ready, if necessary.
  - **Secondary Site Leader Readiness Check Timeout (minutes):** The amount of time a secondary site member waits for its leader to be ready to download the database. After this amount of time, the secondary site member directly downloads the database from the primary site instead of through its site leader. The default setting is 30 minutes.
8. **Cluster Members:** List all the cluster member IP addresses.  
For guidance on cluster size, see the section about [Set Up a Cluster](#) page.
- **Member Address:** Enter the local IP address, AWS VPC IP, or FQDN.
  - **Member NAT Address/FQDN:** Enter mapped addresses in the form NAT, AWS EIP, or FQDN.
- All cluster members are synchronized automatically. The list is prioritized as follows:
- a. The first member is the source of data during the initial synchronization, and referred to as the "replication leader."
  - b. If the first member ever fails, the second member in the list becomes the new replication leader.
  - c. The up and down arrows move the selected IP address position in the order of the list. These buttons are visible only for the primary site.
  - d. The **X** immediately deletes the selected IP address.
9. Select **OK** to save the cluster site configuration.

## Other Steps

Once you have added a cluster site, follow these steps:

1. Select **Save Config Locally** to save the cluster configuration to the local appliance.
2. Select **Save To Cluster** to save the cluster configuration to all members in the cluster.

### NOTE

If you intend to enable cryptography for stored credentials, do so before turning on the cluster. See [Configure Enhanced Encryption for Stored Credentials](#) for instructions.

3. Select **Turn Cluster On**.

### WARNING

The *first time* that you turn on a cluster, start it at the first member in the primary site. The first member is the replication leader. Later, you can start the cluster from any member in the primary site. You can turn off a cluster from any member in the cluster, including secondary site members.

Any sessions from Secondary site members are logged off when the cluster starts. Sessions from Primary site members are interrupted but can be resumed after the cluster has completed its startup.

The **Cluster Startup Details** window appears with the following information:

- **Primary Site Members:** The number of primary site members appears in brackets, followed by a progress bar that advances as primary site members are synchronized.
- **Primary Site Leaders:** The number of secondary site leaders appears in brackets, followed by a progress bar that advances as secondary site leaders are synchronized.
- **All Members:** The total number of cluster members appears in brackets, followed by a progress bar that advances as cluster members are synchronized.
- **Countdown to Refresh:** Every 10 seconds the status refreshes. This counter lets you know that status is still being communicated.
- **Message Box:** The IP address and site name of each member appears. Status messages appear for each member as progress is updated.

When synchronization is complete for all primary members and each secondary leader, the cluster is ready to accept traffic. Other secondary members continue to synchronize while other members are available.

Once all cluster members are in sync, the Cluster Startup Details window disappears. The Status tab takes focus, displaying sites and the status of all site members.

### NOTE

In clusters, the blue globe icon on the title of a configuration panel signifies that the configuration is global, and replicated to all cluster members.

### NOTE

For more information see the following topics:

- [Add a Cluster Member](#)
- [Cluster Synchronization, Promotion, and Recovery](#)

## Add a Member to a Site While the Cluster is Up

This procedure describes how to add a member to the primary site or a secondary site of a cluster while it is up.

### NOTE

Adding a PAM instance to a cluster overwrites its data with cluster data, except for local configurations. Because credentials are included, you should log in as a user with the configuration management role that exists in both places, such as *super*. Keep in mind that the credentials overwrite and may be different.

**To add a cluster member, follow these steps:**

1. Ensure that the new PAM instance meets the requirements that are given in [Cluster Deployment Requirements](#).
2. On an existing cluster member, copy the **Shared Key** from the **Configuration, Clustering** page, **Local Settings** tab. If you know the **Passphrase**, you can enter it on the new member instead. **Note:** If you are in FIPS mode, the Passphrase is not used.
3. On the same page, see which **Interface** clustering is using (such as GB2).
4. On the new cluster member, go to the **Configuration, Clustering** page, **Local Settings** tab. Paste or **Generate** the **Key** and select the **Interface**. **Note:** If you are in FIPS mode, the **Generate Key** button is disabled.
5. Select **Save Config Locally**.
6. On the **Global Settings** tab, select **Load Configuration from Member**.
7. In the resulting window, enter the IP address of an existing member of the cluster, and select **OK**. The **Clustering** page gets information from the existing member and displays it.
8. Select a Primary or Secondary site and **Update**. To add a new site, see [Add a Cluster Site](#). The Update Cluster Site window appears.
9. Select **+** (Add a cluster member) to join it. Enter at least the first field value:
  - **Member Address:** Enter the local IP address, AWS VPC IP, or FQDN.
  - **Member NAT Address/FQDN:** Enter mapped addresses in the form NAT, AWS EIP, or FQDN.
  - **NAT Port:** Enter the NAT port, if applicable.
10. Select **OK**.
11. Select **Subscribe to Active Cluster**, and select **Yes** to join the active cluster when prompted. The new cluster member begins synchronization by pulling data from the cluster site leader. PAM restarts on the new cluster member. When the new cluster member finishes its sync with the Primary or Secondary leader, you can log in again.
12. On the **Configuration, Clustering** page, the Status tab displays information about the cluster:
  - Primary Site members display all sites and cluster members.
  - Secondary Site members list all sites but displays only their own member information.

**NOTE**

[Cluster Synchronization, Promotion, and Recovery](#)

**Change the IP Address of a Cluster Member**

If your network infrastructure changes, you might need to change the IP address of a cluster member. This procedure ensures proper operation of the cluster after a change to the IP address of a member.

**Follow these steps:**

1. Log in to the cluster member whose IP address you want to change.
2. Turn clustering off by selecting **Configuration, Clustering** and selecting **Turn Cluster Off**.
3. Navigate to **Configuration, Network, Network Settings**.
4. In the Network Interfaces list, select the interface that you want to modify and change the IP address.
5. Select **Update**.
6. Reboot the cluster member by selecting **Configuration, Power**, then selecting **Reboot Instance**.
7. After the cluster member reboots, log back in to the updated cluster member.

**NOTE**

If the cluster member has only one interface IP address, use the updated IP address in the URL to log back in to the instance.

8. Navigate to **Configure, Clustering, Global Settings**.
9. From the Sites list, select the entry for the site with the updated cluster member and select **Update**.
10. Change the IP address to the new address.

11. Select **Save Config Locally** followed by **Save to Cluster**.
12. Restart the cluster by selecting **Turn Cluster On**.

The cluster resumes operation with the updated address of the member.

## Tune a Cluster

Use cluster tuning *only* with the direction of Broadcom Support. To change configuration items that are not already visible on the Clustering page, follow these steps:

1. Verify that the Cluster is off.
2. Go to the **Configuration, Diagnostics, System** page.
3. Find **Cluster Tuning Mode**. Select the **On** button.
4. Go to the **Configuration, Clustering** page.
5. Select the **Tuning** tab.
6. Inspect and modify the following settings as directed by Broadcom Support:
  - **Enable Cluster Status Replication Timestamps:** When you select this option, two more columns appear for Site Members on the Status tab. A replication sample is sent from each member every minute. The column values are updated every five minutes. Select the **Refresh Replication Status** button to update the status immediately. These times will usually not differ between Primary Site members that are sending to and from each other, due to group replication.
    - **Last Replication Sample Received:** The elapsed time since this member last received a replication sample from the primary site or secondary leader.
    - **Last Replication Sample Sent:** The elapsed time since this member last sent a replication sample to the primary site or secondary leader.
  - **Duration to Preserve MySQL Binary Logs (hours):** Replication uses these logs to keep secondary sites in sync. If a secondary site goes further out of sync than logs are available, the entire database must be delivered to the site. The default value is 24 hours.
  - **Time of Day to Perform Log Trim and DB Dump:** The UTC time to perform this action.
  - **Primary Member Recovery Period (hours):** If a primary site member goes further out of sync than this period, the entire database must be delivered to the member. The default value is 24 hours.
  - **Cluster Database Consistency Check Period (minutes):** Configure how often, in minutes, the sync status is updated across the cluster. The default value is 5 minutes.
  - **Allowed Replication Lag Before Secondary Member Warning (minutes):** When a Secondary member loses connectivity with the primary site, it receives a warning after this duration.
  - **Allowed Replication Lag Before Secondary Member Out-of-Sync (minutes):** When a Secondary member loses connectivity with the primary site, it is marked Out-of-Sync after this duration.
  - **Allowed Replication Lag Before Secondary Member Deactivation (minutes):** When a Secondary member loses connectivity with the primary site, it is marked as Deactivated after this duration.
  - **Database Connection Timeout (minutes):** If the primary site cluster members detect quorum loss, wait for this duration before initiating quorum loss mode. If you set this value too low, you risk false alarms. Switching into quorum loss mode and back is time-consuming.

## Clustering Considerations for Appliances with Multiple Network Interfaces

If you have a clustered environment in which your PAM appliances have multiple network interfaces, configure you cluster as described in the previous pages then follow this procedure to avoid replication failures. These replication failures result from firewall rules that PAM creates to protect MySQL cluster replication traffic. If any cluster-to-cluster communication is sent using the wrong network interface (and therefore the wrong IP address), PAM replication fails because the proper firewall rules are not opened up.

## What to Check for Prior to Starting Your Cluster

To verify that your network interface controllers (NICs) are properly configured, first contact Broadcom Support to enable *Debug SSH*.

Once debug SSH is enabled, follow these steps:

1. SSH into every member of every site in your cluster.
2. From the SSH session for the primary leader, run the `ip route` command against *each* of the other members of that site:

```
ip route get intra-cluster-ip-address
```

3. From the SSH sessions of *each* of the other members of the primary site run the `ip route` command against the inter-cluster addresses of each member of the secondary sites:

```
ip route get secondary-site-member-inter-cluster-ip-address
```

4. From the SSH sessions of each of the members of the secondary sites, run the `ip route` command against each of the into cluster members of the primary site.

```
ip route get primary-site-member-inter-cluster-ip-address
```

Here is an example of an `ip route` command output, with the important content shown in bold:

```
# ip route get 10.242.2.160
10.242.2.160 via 10.236.12.1 dev eth0 src 10.236.12.241
cache
```

This IP address in bold indicates which of that IP addresses of that machine is used to initiate communication to the destination machine. If the significant IP address is the same as what is specified in your cluster configuration, then there is no problem. If the significant IP address is *not* the same as what is specified in your cluster configuration, then either your cluster configuration is in error or your additional routes are in incorrect.

## What To Do If Your Routes Are Incorrect

Additional routes are specified in the PAM configuration. If your routes are wrong, you can view the ones actually in effect using the `route` command. For example:

```
# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
default          10.236.12.1     0.0.0.0          UG    0      0      0 eth0
10.236.12.0      0.0.0.0         255.255.254.0    U      0      0      0 eth0
10.236.16.0      0.0.0.0         255.255.254.0    U      0      0      0 eth7
10.242.4.0       10.236.16.1     255.255.254.0    UG     1      0      0 eth7
localhost        0.0.0.0         255.255.255.255 UH     0      0      0 lo
```

This shows the routes actually in effect, the corresponding gateway, and the network interface that is be used. The network interfaces are described in linux terms. To correlate these to PAM terms, run the `/sbin/interfaceMappings.sh` command. For example:

```
# /sbin/interfaceMappings.sh
BOND1=bond0
BOND2=bond1
BOND3=bond2
BOND4=bond3
GB1=eth0
GB2=eth1
GB3=eth2
GB4=eth3
```

```
GB5=eth4
GB6=eth5
GB7=eth6
GB8=eth7
```

This example shows you that linux interface eth0 corresponds to PAM interface GB1 and that eth7 corresponds to GB8.

To see the IP addresses corresponding to each of these, run the `ipconfig` command. For example:

```
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.236.12.241 netmask 255.255.254.0 broadcast 10.236.13.255
    inet6 fe80::290:bff:fe43:1cf4 prefixlen 64 scopeid 0x20<link>
    ether 00:90:0b:43:1c:f4 txqueuelen 1000 (Ethernet)
    RX packets 234011558 bytes 291206046553 (271.2 GiB)
    RX errors 0 dropped 25393 overruns 0 frame 0
    TX packets 106480688 bytes 32363304465 (30.1 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0xf7a00000-f7afffff

eth7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.236.16.21 netmask 255.255.254.0 broadcast 10.236.17.255
    inet6 fe80::290:bff:fe43:1cfb prefixlen 64 scopeid 0x20<link>
    ether 00:90:0b:43:1c:fb txqueuelen 1000 (Ethernet)
    RX packets 12763590 bytes 5259011456 (4.8 GiB)
    RX errors 0 dropped 231 overruns 0 frame 0
    TX packets 12319523 bytes 5132833296 (4.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0xf6500000-f65fffff

eth7:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.236.16.24 netmask 255.255.254.0 broadcast 10.236.17.255
    ether 00:90:0b:43:1c:fb txqueuelen 1000 (Ethernet)
    device memory 0xf6500000-f65fffff

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 309661353 bytes 301153155953 (280.4 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 309661353 bytes 301153155953 (280.4 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The previous example shows that eth0/GB1 has IP address 10.236.12.241, and that eth7/GB8 has address 10.236.16.2

Once you have established the correct routes, configure them using **Configuration, Network, Additional Routes** in the PAM UI.

For more information, see [Additional Routes](#)



## Cluster Synchronization, Promotion, and Recovery

After your cluster is configured and turned on, the **Status** tab on the **Configuration, Clustering** panel shows a list of cluster sites and members and details about each. The view of a cluster varies depending on whether you are logged in to a Primary site member or a secondary member.

From the **Status** tab, you can perform the tasks described in this topic.

### View Member Status

Each cluster member lists its status in the Site Members section of the clustering **Status** tab. On Primary site members, members of all sites are visible. On Secondary site members, only that member is visible. Primary site replication is evaluated every minute. Secondary replication status is evaluated every 5 minutes. Select **Refresh Replication Status** to update the status immediately. When a new member subscribes to a cluster, its database status is unknown. The status columns might appear out of alignment. Select the **Refresh Replication Status** button to update its status. Because the **Status** tab does not update automatically, you can use the **Refresh** button to update the UI.

### **Primary Site Members**

For the primary site, replication status updates every minute. If a member status is anything but "online" or "recovering", a warning indicator appears on the **Site Members** table, and an email notification is sent to the monitor. Monitor settings (**Configuration, Monitor**) are not replicated, so each primary member needs the email set separately. Each member should have the same monitor settings.

**Site Member Active:** Primary sites are always active.

**Replication Status:** A green checkmark indicates that the member is online and in sync. A yellow triangle with an exclamation mark means that the member is "recovering," is lagging, or communication has timed out. A red X indicates that the member status is offline, unreachable, error or missing, or out of sync. Hover over the icon to see a tooltip explaining the reason.

### **Replication Detail:**

- **Online:** The member is a fully functional group member, can connect and start executing transactions.
- **Recovering:** The member is going through the recovery process, receiving state information from a donor.
- **Offline:** MySQL exists on the member, but it does not belong to the group.
- **Unreachable:** The group suspects that the server is not reachable because it has crashed or disconnected involuntarily.
- **Error:** An error occurred on the recovery phase or while applying changes.
- **Missing:** Privileged Access Manager cannot find the member in the MySQL replication group.

**Log Files:** Every minute, sample data is replicated among primary site members. The cluster status log records the time that has elapsed since the last sample was sent and received (as mm:hh:ss). See [View Cluster Logs](#) for more information.

### **Secondary Site Members**

**Site Member Active:** A green checkmark indicates that the member is active. A red X indicates that the member has been deactivated. Secondary sites can be deactivated if they lag in replication more than 15 minutes behind the primary site. This threshold is configurable on the Tuning tab, but should only be done with the assistance of Broadcom Support. See [Cluster Tuning](#) for more information.

**Replication Status:** A green checkmark indicates that the member is online and in sync. A yellow triangle with an exclamation mark means that the member is lagging, or communication has timed out. A red X indicates that the member status is inactive or out of sync. Hover over the icon to see a tooltip explaining the reason.

**Replication Detail:** These thresholds are configurable on the Tuning tab, but should only be done with the assistance of Broadcom Support. See [Cluster Tuning](#) for more information.



- **In Sync:** Member is in sync with the primary site.
- **Timeout:** A yellow triangle with an exclamation mark means that the connection has timed out trying to contact this member. A warning appears on the Site Members table.
- **Lag Detected:** The member lags 5 minutes behind the Primary Site. A warning appears on the Site Members table.
- **Out of Sync:** The member lags 10 minutes behind the Primary Site. A warning appears on the Site Members table.
- **Inactive:** The member lags 15 minutes behind the Primary Site. When Inactive, a member no longer allows password views, auto-login, and so on. An email is sent to the Monitor. **Important:** When you change this value, you are changing how far out of sync a member can get before stopping it from functioning. However, if the Primary Site is unavailable and it is set to Operationally Safe mode, the Secondary Site can serve its own stale data. See step 5 in [Configure a Cluster](#).

**Log File:** Every minute, sample data is replicated from the primary site to secondary sites. Every 5 minutes, the cluster status log records the time that has elapsed since the last sample was received (as mm:hh:ss). Every minute, sample data is also replicated from the secondary site to primary site. Every 5 minutes, the cluster status log records the time that has elapsed since the last sample was sent (as mm:hh:ss). See [View Cluster Logs](#) for more information.

## **Remove Cluster Members**

### ***Primary Site***

From a Primary Site member, you can remove a member from any site without stopping the cluster. Select the member in the Site Members table on the **Status** tab and select **Eject Member**. This operation causes a dynamic reconfiguration of the cluster, and does not launch a recovery process.

#### **NOTE**

Ejecting a primary site member while jobs are running on that member terminates the jobs. To protect against such unintended consequences, put the member in Maintenance Mode and wait for it to quiesce before ejecting it.

### ***Secondary Site***

On a Secondary Site member, you can remove a member that you are viewing by using the **Leave Cluster** button. The **Leave Cluster** button lets you remove a secondary member from a cluster while the cluster remains on. This operation causes a dynamic reconfiguration of the cluster, and does not launch a recovery process. If it is the Secondary leader, the next member in the Secondary site becomes the site leader. However, you cannot remove the last remaining member of cluster. In that case, you must delete the site using the **Delete** button. You can also remove or add a Secondary Site without stopping the cluster.

## **Stop the Cluster**

To stop an entire cluster, select **Turn Cluster Off**. You can turn off a cluster from a primary or secondary member.

## **View Cluster Logs**

For troubleshooting purposes, review the cluster logs. Select **View Cluster Logs** from the primary or secondary members. On a secondary member, only the local site cluster logs are accessible.

The View Cluster Logs button is also available on the Global Settings tab when it is not enabled on the **Status** tab.

## **Cluster Synchronization**

Site members can get out of sync, particularly when a site member becomes unavailable. When you synchronize a cluster, databases across all members are updated.

**NOTE**

The re-sync process to a Secondary site or individual member downloads the entire database and terminates any active sessions on the Secondary site or member. Because re-syncing disrupts active user sessions on the member nodes that are involved, place the member nodes that are involved in the resync into maintenance mode for some time before the re-sync to prevent user logins to the affected nodes. For related information, see [Enable Maintenance Mode](#) under [Maintenance and Cluster Tuning Options](#).

**Synchronizing Sites**

The Sites section of the **Status** tab lists the Site Name, Type (primary or secondary), VIP IP address, and VIP FQDN.

The **Re-sync Site** button lets you synchronize all members at a given secondary site. You cannot re-sync a primary site. You cannot re-sync a secondary site unless it can contact the primary site.

**To re-sync a site:**

1. Select the checkbox next to the site you want to re-sync. Re-sync sites one at a time.
2. Select **Re-sync Site**.

**Synchronizing Site Members**

When clustering is on, the list of members differs depending on whether you are logged in to a member of a primary or secondary site:

- On a primary site member, the Site Members section shows the members for all sites.
- On a secondary site member, you can only see the secondary member that you are logged in to.

Individual secondary site members can be re-synced from any primary member. You can also re-sync a secondary member by directly logging in to that secondary site member.

**To re-sync a site member:**

1. Select the checkbox next to the member you want to re-sync.
2. Select **Re-sync Site Member**.

**Refresh Site Member Databases**

In the Site Members section, you can see the status of the member databases. To refresh the database status, use the **Refresh Replication Status** button. The elapsed time since the last sample replication was received, and the time since the last sample replication was sent is listed for secondary members.

**TIP**

On a primary site member, selecting the Refresh buttons updates the database status of all the members in the entire cluster.

**Secondary Member Rejoins the Cluster**

If an unreachable secondary site member comes back online, the member tries rejoining the cluster. First, the member asks the secondary leader for a copy of its database. The member performs an integrity check on the data, then uses it to overwrite its own data. After that check is complete, the database starts. Finally, the cluster recognizes this member, and user logins are forwarded to this member.

**Databases During Synchronization**

When a cluster starts, Privileged Access Manager takes a snapshot of the primary site database. The primary replication leader is the first one in the primary site member list. The replication process applies this snapshot to each of the cluster members, and reports site members as active. If the primary database is not active at the start, the database remains out of sync and you can lose data ([see this note about deactivated databases](#)).

Always start a cluster from a member with an in-sync database. To determine whether its replication status is in sync, look at the Site Members list.

If the primary database is not active, follow these steps:

1. Note the database status for each member.
2. Reorder the cluster members so that a primary member with an active database is reassigned to the top of the list.
3. Restart the cluster:
  - a. On the **Status** tab, select **Turn Cluster Off**.
  - b. On the Global Settings tab, select **Turn Cluster On**.

### **Primary Site Recovery**

Privileged Access Manager uses MySQL group replication for the cluster primary site, and traditional master-slave replication to and from secondary sites.

In MySQL group replication, a "quorum" is the number of members that are required to make decisions for the cluster, such as member health. The quorum is the majority of the members in a cluster, or in this case the Primary Site. The quorum for a three-member primary site is two, and for five members, the quorum is three. The quorum requirement prevents a "split-brain" scenario, where cluster members that are isolated (through network or power failure, for example) could continue operating separately.

If you remove a primary site cluster member voluntarily and gracefully, the cluster is dynamically reconfigured, producing a new quorum. A graceful (or orderly) shutdown is one of the following methods, rather than an abrupt shutdown:

- Use the **Configuration, Power, Stop Instance** control.
- On the **Configuration, Clustering** page in the UI, select the member in the Site Members table on the **Status** tab. Select **Eject Member**.
- On VMware, use the PAM Utility Console. Select **Power off PAM**.

For example, a four-member primary site cluster has a quorum of three. If you eject a member, the resulting three-member cluster has a quorum of two. See the [Fault Tolerance](#) chart for details.

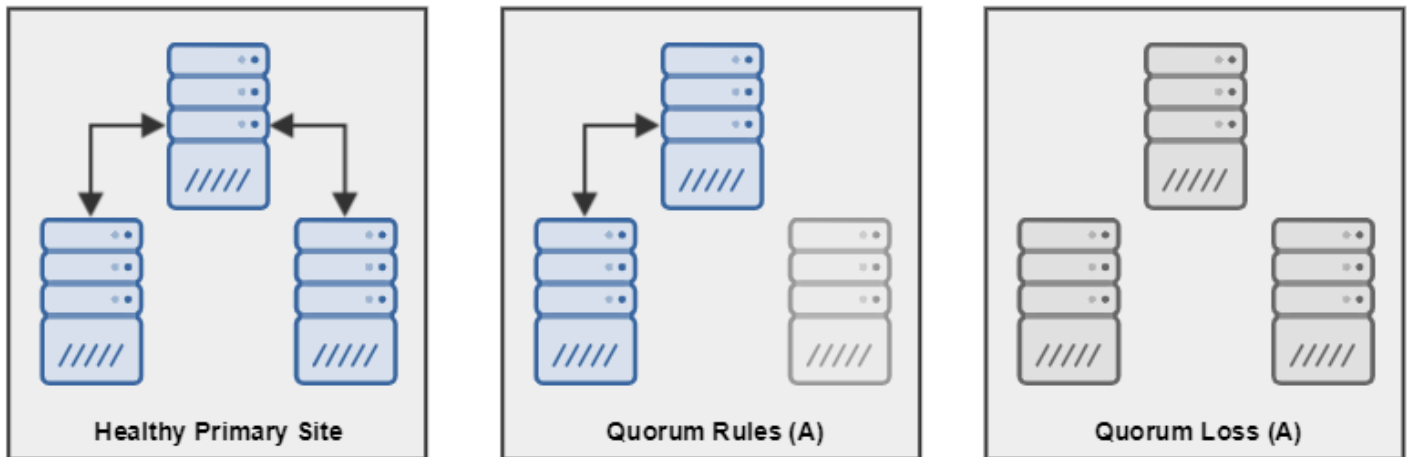
### ***Quorum Loss Example***

Consider a primary site cluster with three members. One member becomes inaccessible because of a network failure. The cluster continues, and alerts administrators that one member is unavailable. If someone reboots a second member, a quorum cannot be achieved. Quorum loss requires PAM administrator intervention at this point, even if one of the members revives itself. See [Quorum Loss](#) for more information.

If the second member had been gracefully removed, as described in [Primary Site Recovery](#), the cluster would have dynamically reconfigured itself. No quorum loss would have been encountered.

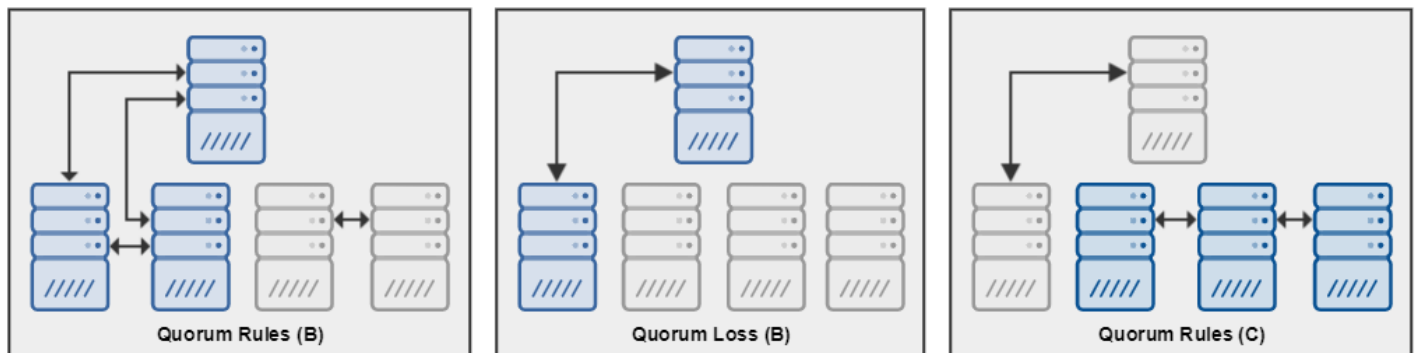
### ***Quorum Loss Diagrams***

The following diagram illustrates a three-member Primary Site of a cluster in three different situations. Descriptions of the situations follow the illustrations.



The following diagram illustrates a five-member Primary Site of a cluster in three different situations. Descriptions of the situations follow the illustrations.

**Figure 17: Quorum by 5**



### **Healthy Primary Site**

In a healthy primary site, all members can communicate with each other. Replication proceeds uneventfully.

### **Quorum Rules**

If a primary site member cannot be reached by other members, the remaining members try to form a quorum. With a quorum, the remaining members continue to operate as a cluster. See the [Fault Tolerance](#) chart for details.

The preceding illustrations show three examples of a quorum continuing even though members have been lost. A power failure, network partition, or hardware failure could cause this disruption.

- In *Quorum Rules (A)*, one member is not reachable from the other two. Because two members can communicate, and they constitute a majority, they continue operating as cluster members. The odd member, if operational, cannot contact the others, therefore it ceases to operate as a cluster member. The instance then goes into [cluster recovery](#) mode.
- In *Quorum Rules (B)*, a network partition has divided the cluster members. Although two members can communicate with each other, they cannot form a quorum. The other three members make a quorum, and so continue as the cluster.
- In *Quorum Rules (C)*, a network partition has divided the cluster members. The primary replication leader can only contact one member, while three other members can communicate among themselves. Those three members make a quorum, and so continue as the cluster.

### **Cluster Recovery**

When one or more cluster members cannot join a quorum, the following actions are taken:

- Turn off clustering on the instance
- Back up its database
- Stop group replication
- Restart the application
- Send email notifications
- Standard login user interface is limited to configuration, including Clustering, Diagnostics, Upgrade, and Power
- If that member is managing the load-balancing VIP, the next available member in the list takes up that responsibility.

The cluster member attempts to heal itself in the following manner:

- Determine the replication leader by finding the member with the latest transaction
- Reboot itself if it is not the leader, up to five times

### **Quorum Loss**

Without a quorum, group replication cannot determine who has the latest complete data. A PAM administrator can log in to a primary site member to determine the next course of action:

- **Resume Cluster:** Reboot all cluster members for self-healing
- **Eject Member:** Remove an instance from the cluster. You can then diagnose and repair it apart from the cluster. Ejecting members from the Primary Site effectively reconfigures the number of members in the site. For example, in *Quorum Loss (B)*, if the cluster administrator ejects the unresponsive members, the remaining members make up the new cluster and can continue. This action risks losing data that could reside on the unresponsive members.

### **Member Rejoins the Cluster**

When a primary site member is unreachable, it no longer handles any load balancing. To remedy this problem, restart the cluster, but note the following caveat:

#### **WARNING**

If the first primary site member in the primary site list has an out-of-sync database, do not start the cluster. If you start a cluster from member with an out-of-sync database, you can lose data. To avoid this problem, reorder the primary site members in the list. Make the member with the first in-sync database (green checkmark) the first member in the list. Restart the cluster from this first member, which becomes the primary replication leader. If you have questions, contact Broadcom Support.

### **All Primary Members are Down**

For an active cluster (turned on), an event can occur to cause all members of the primary site to stop working. Events such as a power failure might cause the operating system of each site member to stop. When all the members come back online, the state of the cluster is unpredictable.

**To restore cluster stability, follow these steps:**

1. Turn off the cluster.
2. Determine which primary site member is the most trusted and up-to-date. See [Replication Analysis](#). That member might be the one that failed last relative to the other members.
3. Reorder the most trusted member to the first member in the primary site list.
4. Restart the cluster from this first member.

### **Site Promotion Using Replication Analysis**

In a multi-site cluster, if the Primary site is unavailable, you must promote a Secondary site to become the Primary site. Ideally, promote the Secondary site that has the most up-to-date information. For guidance on which Secondary site is the most up to date, use the replication analysis feature.

**NOTE**

Primary site replication IDs can be much higher than secondary site replication IDs because not all transactions are replicated to secondary sites. Replication IDs are also expected to vary slightly among primary site members as they continually update. This behavior is normal and should not affect secondary site promotion decisions. Replication Analysis is not intended to monitor ongoing replication activity.

**To promote a secondary site, follow these steps:**

1. Go to **Configuration, Clustering** page, **Status** tab and select **Turn Cluster Off**.  
A warning appears. Once you accept it, a "Turning Cluster Off" message appears.
2. Go to the **Global Settings** tab and select **Replication Analysis**.  
The Replication Analysis window opens. The page lists the site name, cluster member, and last replication ID for that member.
3. Determine the site and member with the highest replication ID, then close the page.
4. Select the site with the highest ID, then select **Set Primary Site**.
5. Move up the member in the new primary site to the first position in the list.
6. Select **Save Config Locally**.
7. Select **Save to Cluster**.  
When you promote a secondary site, saving the cluster might fail. To solve this problem, remove the site that is no longer reachable and save.
8. Select **Turn Cluster On**.
9. If you use the REST API or CLI Commands, ensure that they point to the VIP of the new primary site.

**NOTE**

The order of the sites Global Settings page remains the same even after you promote a site. The primary site is not always listed first. The first member in the newly promoted site is the new replication leader. Look at the Type column to determine primary and secondary sites.

**Unlock a Member When the Cluster Is Off**

When the cluster is turned off, the Credential Management services of each member are locked. No credentials can be viewed or used in auto-connect. An **Unlock Me** button is available on the **Status** tab. An unlocked member is independent of the cluster replication process, and can cause synchronization problems.

Before you unlock a member, note the following points:

- Unlocking permits scheduled jobs and processes to continue, which can trigger credential rotation.
- If the unlocked member is not the primary member of the cluster, any changes are lost after the cluster restarts.

**Application Distinct from Replication Leader**

The primary replication leader is elected by MySQL to be the source of data replication. The "application master", on the other hand, is elected by the Privileged Access Manager application. The application master is responsible for credential management jobs that rotate passwords. This member might not be the same as the primary replication leader.

If a standard user logs out from a secondary site member, a password rotation is handled by the application master in the primary site. If the application master shuts down, another primary site member is elected by PAM.

**NOTE**

- [Cluster Maintenance](#)
- [Cluster Backup and Disaster Recovery Process](#)

## Primary Site Fault Tolerance

In a PAM cluster, the Primary site makes fault tolerance decisions that are based on its quorum. For more information about the quorum, see [Primary Site Recovery](#). The size of the Primary site determines the quorum. The quorum determines its fault tolerance, or how many members the Primary site can lose and continue normal operations.

To ensure Primary site fault tolerance, we recommend at least three members at a Primary site. If the entire cluster has only two members, do not put both members in the Primary site. We recommend a 1 x 1 configuration (one member at the Primary site and one member at Secondary site).

Primary Site Size	Quorum	Member Failures Tolerated
1	1	0
2	2	0
3	2	1
4	3	1
5	3	2
6	4	2
7	4	3
8	5	3
9	5	4

## Configure Load Balancers to Determine the Availability of Cluster Nodes

Privileged Access Manager provides a health verification script ([https://PAM\\_server/health.php](https://PAM_server/health.php)) that load balancers can poll to determine the availability of nodes in your cluster. If the node is operating correctly, `health.php` returns HTTP status code 200 OK.

If any of the following problem conditions apply, the script returns HTTP status code 503 Service Unavailable:

- The node is in maintenance mode.
- Clustering is ON, the node is a secondary site member which is not active
- Clustering is ON, the node is a secondary site which is out of sync with the primary node
- The node is locked.

### NOTE

For information about unlocking nodes, see the section titled "Unlock a Member When the Cluster Is off" in the [Cluster Synchronization, Promotion, and Recovery](#) topic.

## Install and Configure a Socket Filter Agent

Privileged Access Manager Socket Filter Agents (SFAs) can restrict access to and from server-based devices. Socket filters provide a different kind of access control than devices with finite command sets, such as routers, for which command filtering is applied.

SFAs work with Socket Filter Lists (SFLs) configured on the PAM server. For details, see [Socket Filter Agent Support](#).

### Socket Filter Agent Installation Requirements

This section describes SFA requirements for installing a Socket Filter Agent.

- **Network Port Requirements:** SFAs have the following network port requirements:

- By default, port 8550 must be allowed between the target host containing the SFA and the appliance. You can configure the SFA to use a different port.
- Port 443 must also be open to allow communication back to the appliance, including messages for log entries.

**NOTE**

For AWS or Azure, ensure that these ports are also open in the AWS or Azure network settings, and the OS firewall of the instance.

- **Permissions:** SFA installation requires administration privileges, such as those provided by the Windows default Administrator account or the UNIX `root` account.
- **Supported Operating Systems:** See [Supported Environments](#) for operating systems that support the SFA.

Use the following optional procedure to monitor the status of SFA agents from the PAM UI.

**Download the Socket Filter Agent Software**

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

**Install and Configure a Socket Filter Agent on Windows**

Windows Socket Filter Agents are provided as MSI self-extracting packages. This section describes how to install and configure SFAs on a Windows target system.

**NOTE**

On Window targets, Socket Filter policies are not enforced against users who log in to targets directly, bypassing Privileged Access Manager.

***Install a Windows SFA Using the Installer UI***

Use this procedure to install a Windows SFA using the installer UI.

The account that is used to install the SFA impacts which accounts can uninstall the SFA. If one of the following accounts installs the SFA, no other account can uninstall the agent:

- A domain-based account with local Administrator privileges
- A local account with local Administrator privilege installs the SFA, but not the Administrator itself.
- A local Administrator account with local Administrator privileges

If the installing domain-based or local account becomes obsolete or invalid, you might not be able to uninstall the SFA. To uninstall the SFA product under these circumstances, contact Broadcom Support.

**Follow these steps:**

1. Ensure that all installation prerequisites are met.
2. Log in to the target Windows device as a local administrator.
3. Use the **Add/Remove Programs** window (or equivalent) to remove any existing Windows SFA from the target device.
4. Navigate to the directory where you uncompressed the SFA download.
5. Start the installer by double-clicking the `WinSFA.exe` file.
6. Follow the prompts.

After installation, the SFA starts and runs as a background Windows service with the default name "CA Technologies Socket Filter". Use the local Windows Services interface for service settings and control.

***Install an SFA Silently on Windows***

Use this procedure to install a Windows SFA silently with automatic startup.



The account that is used to install the SFA impacts which accounts can uninstall the SFA. If one of the following accounts installs the SFA, no other account can uninstall the agent:

- A domain-based account with local Administrator privileges
- A local account with local Administrator privilege installs the SFA, but not the Administrator itself.
- A local Administrator account with local Administrator privileges

If the installing domain-based or local account becomes obsolete or invalid, you might not be able to uninstall the SFA. To uninstall the SFA product under these circumstances, contact Broadcom Support.

#### Follow these steps:

1. Ensure that all installation prerequisites are met.
2. Log in to the target Windows device as a local administrator.
3. Use the **Add/Remove Programs** window (or equivalent) to remove any existing Windows SFA from the target device.
4. Navigate to the directory where you uncompressed the SFA download.
5. Open a Command Prompt window and navigate to the directory where you uncompressed the SFA download.

#### NOTE

On Windows Server 2008 and Windows Server 2012, right-click on the Command Prompt icon and select **Run as Administrator**.

6. Enter the following command:

```
path\WinSFA.exe /s /v"/qn /liwe c:\XCDM_SFA.log"
```

Where *path* is the path where the WinSFA.exe file is located.

The /q and /l options and parameters are recommended but not required.

After installation, the SFA starts and runs as a background Windows service (with the default name "CA Technologies Socket Filter"). Use the local Windows Services interface for service settings and control.

#### Change Basic Windows SFA Configuration Settings

Run the SFAConfig.exe configuration utility to change basic SFA settings.

#### Follow these steps:

1. Navigate to *SFA\_Install\_Dir*\Bin.  
*SFA\_Install\_Dir* is the SFA installation directory. Default: C:\Program Files (x86)\CATech\Socket Filter.
2. Execute *SFAConfig.exe*.
3. Change any of the following settings, as required:
  - **Port:** The port that the SFA uses to communicate with the appliance. Default: 8550
  - **Service Name:** The name of the SFA Windows service. Default: "CA Technologies Socket Filter."
  - **Service Description:** The description of the SFA Windows service Default: "CA Technologies Socket Filter."
  - **Run Agent in Verbose mode:** If enabled, the SFA produces detailed log messages for diagnostic purposes. Default: off.
  - **Enable IPv6 Protocol:** Set this option to enable the SFA to support IPv6. If not set (the default), the SFA supports only IPv4.
4. Select **Save and Restart Service**.  
The SFA restarts and the configuration changes are implemented.

#### Reconfigure a Windows SFA to Use Changes to the Target Device Network Configuration

The SFA reads and uses the target device network configuration during startup. It does not dynamically update if you make subsequent configuration changes (for example, adding a NIC or changing the IP address). You must therefore restart the SFA to reconfigure it to use target device network changes made *after* startup.

To restart the Windows SFA, use the local Windows Services interface. The default service name is "CA Technologies Socket Filter."

## Troubleshoot a Windows SFA

Turn on Verbose mode using the SFAConfig.exe configuration utility to generate detailed log messages.

Log messages are stored in the `log.txt` file that is located in the installation directory.

## Uninstall a Windows SFA

To uninstall a Windows SFA, do *one* of the following steps:

- Access the Windows Control Panel and use the **Add/Remove Programs** window (or equivalent).
- Open a Command Prompt window and enter the following text:

```
MsiExec.exe /X{5A2A2643-2BD6-4D09-9B03-E08098887B06} /norestart
```

## Install and Configure a Socket Filter Agent on UNIX

This section describes how to install and configure a Socket Filter Agent (SFAs) on a UNIX target.

### NOTE

On UNIX and Linux targets, the Socket Filter Agent only filters non-root users. A Socket Filter List in a policy becomes effective only for non-root users logging in to targets through PAM. Afterwards, the filter is in effect, even if the user logs in to the target directly. Socket filters for all users are reset after root restarts the socket agent (gksfd).

## Install a UNIX SFA

The UNIX SFA download package contains a separate installer script for each supported UNIX operating system. Each script has a descriptive filename of the following format:

```
gksfd_sfa-version_os-version[_64]_linux_install.sh
```

Where *sfa-version* is the SFA release version and *os-version* is the UNIX version.

For example:

- `gksfd_4.1.7_debian6_64_linux_install.sh` for a Release 4.1.7 SFA for Debian 6 (64-bit)
- `gksfd_4.1.7_rh6_linux_install.sh` for a Release 4.1.7 SFA for Red Hat EL 6 (32-bit)

### NOTE

You can use `gksfd_.xx_rh7_linux_64_install.sh` to install Red Hat Enterprise Linux 7, 8, and 9 systems.

Depending on the OS, there are different methods of deploying the SFAs. Because minimal configuration is required on the managed target device, an SFA can be deployed through preexisting software delivery mechanisms.

## Follow these steps:

1. Ensure that all installation prerequisites are met.
2. Log in to the target device as a local administrator.
3. Remove any existing UNIX SFA from the target device.
4. Open a terminal window.
5. Copy the appropriate installer script for your operating system to the directory where you want to install the SFA.
6. Run the installer script. For example, to install a 4.1.7 SFA on Red Hat Enterprise Linux (32-bit):

```
[root]# sh gksfd_4.1.7
_rh6_linux_install.sh
```

A terminal window opens, allowing you to interact with the installer script.

7. Follow the online directions. When requested, supply a destination directory to install the SFA. The default is `/usr/sbin`.

**NOTE**

Specifying a location different from the default installation location can cause unexpected behavior. We therefore recommend that you accept the default location.

The control script is installed.

**Configure and Operate a UNIX SFA**

A configuration file (`/etc/gksfd.cfg`) and a control script (`rc.gksfd`) control UNIX SFA operation

The following table describes key settings in the `gksfd.cfg` configuration file.

Name	Setting	Description
<b>Login control</b>	<code>SECURE_LOGIN=[ 0   1 ]</code>	0 : Allow login from outside of PAM 1 : Allow login only from a PAM connection.
<b>Secure user list</b>	<code>SECURE_USER= &lt;username_1&gt; , &lt;username_2&gt; , ... &lt;username_N&gt;</code>	Specifies every SFA superuser: every device login user that is not subjected to any socket filter policy.  Each username is delimited with comma, with no spaces permitted.
<b>IPv4 Support</b>	<code>IPv4=[ 0   1 ]</code>	0 : Disable SFA support for IPv4 addresses. 1 : Enable SFA support for IPv4 addresses. (Default)
<b>IPv6 Support</b>	<code>IPv6=[ 0   1 ]</code>	0 : Disable SFA support for IPv6 addresses. 1 : Enable SFA support for IPv6 addresses. (Default)

Use the control script to start, stop, restart, or reload the UNIX SFA process (`gksfd`).

**To run the control script, follow these steps:**

1. Change directory to the installed location of the script on your platform.  
The `rc.gksfd` control script is located in `/etc/init.d/` on all versions of UNIX *except* AIX, HP-UX, and Red Hat Enterprise Linux 9. On those platforms, the control script is installed in the following directories:
  - **AIX:** `/etc/rc.d/init.d/`
  - **HP-UX:** `/sbin/init.d/`
  - **Red Hat Enterprise Linux 9:** `/etc/rc.d/init.d`
2. Launch the control script using the following syntax:

```
rc.gksfd { start | stop | restart | reload }
```

To launch the SFA with options, launch `gksfd` directly using the following syntax:

```
gksfd [-options]
```

The following table describes the options:

Option	Default values when option is not set	Description
-4	N/A	Force the SFA to use only IPv4 addresses.
-6	N/A	Force the SFA to use only IPv6 addresses.

Option	Default values when option is not set	Description
-h		Display online help.
-l logfile	/var/log/gksfd.log	Specify the log file used.
-p port#	8550	Set the port to communicate with the appliance.
-v	info	Set log-level to Verbose mode. For example: /usr/sbin/gksfd -v >> /var/log/gksfdmessages Set this option only when extra logging is required.
-ver		Display the version number.

To apply persistent changes, set the UNIX SFA options in the `rc.gksfd` file.

#### NOTE

Some platforms, such as Red Hat Linux, might block port 8550 by default, which inhibits SFA operation. To determine whether the port is blocked, use the `netstat` command. If necessary, open port 8550 using the command `iptables -I INPUT 1 -p tcp --dport 8550 -j ACCEPT`, and restart the SFA.

### Reconfigure a UNIX SFA to Use Changes to the Target Device Network Configuration

The SFA reads and uses the target device network configuration during startup. The SFA does not dynamically update if you make subsequent configuration changes (for example, adding a NIC or changing the IP address). You must therefore restart the SFA to reconfigure it to use target device network changes made *after* startup.

To restart a UNIX SFA, run the SFA control script as follows:

```
rc.gksfd restart
```

### Troubleshoot a UNIX SFA

Use the `-v` option to turn on Verbose mode to generate detailed log messages.

The default location for log messages is `/var/log/gksfd.log`.

### Uninstall a UNIX SFA

#### Follow these steps:

1. Stop the `gksfd` daemon from the directory where the executable was installed. The following example is for Red Hat 6 Linux:  
[root]# `/etc/init.d/rc.gksfd stop`
2. Delete the following files:
  - The executable, typically located at `/usr/sbin/gksfd`
  - The control script, typically located at `/etc/init.d/rc.gksfd`

## Accessing PAM

Log in to the PAM UI to access the following role-based functionality:

- As a PAM *standard user*, to access and manage privileged network devices.  
For more information about using PAM to access privileged devices, see [Using PAM](#)
- As a PAM administrator, to do the following operations:
  - [Configure PAM servers](#)
  - [Implement PAM network-based access control](#)
  - [Implement Credential Manager to protect privileged account credentials](#)
  - [Implement PAM SC server-based access control](#)
  - [Administrate PAM](#)

### PAM UI Access Methods

End-users and administrators can access the PAM UI using the following methods:

- **PAM Client.** The [PAM Client](#) is an alternative to Internet Explorer that you install on your local workstation. The PAM Client does not interfere with browser-based UI access. Both methods can be used from the same workstation.
- **Web Browser.** Various browsers, such as Chrome, Safari, Edge and Firefox can be used with the following limitations:
  - Microsoft Edge running in Internet Explorer mode is the only browser that still supports NPAPI, which is required to use the RDP and SSH Java applets that are required to access resources. To use Microsoft Edge running in Internet Explorer mode, Java 8u-latest must be installed on the desktop. For more information, see [Internet Explorer mode in Microsoft Edge](#).
  - Microsoft Edge running in Internet Explorer mode does not support the [System Dashboard](#) or the [Management Console Cluster Dashboard](#).
- **PAM Access Agent (Windows only).** The [PAM Access Agent](#) is a lightweight alternative to the PAM Client that you install on your Windows workstation. The PAM Access Agent does not interfere with the browser-based UI access. Both methods can be used from the same workstation.

### Login to the PAM UI Using a Web Browser

To log in to the PAM UI using a supported web browser, follow these steps:

1. Open the browser and navigate to a server URL using *one* of the following formats:

```
https://server_ip_address/
```

```
https://fqdn_of_server
```

*server\_ip\_address* or *fqdn\_of\_server* is the system where you installed the PAM server.

Examples:

```
– https://102.200.11.222/
```

```
– https://capam.forwardinc.com
```

2. At the Login page, enter your credentials.

The credentials are specific to the server. The login experience can be different for the following reasons:

- Single sign-on provisioning might be set up.
- You might have to supply credentials at the point of login to a target system. Your server administrator can tell you if you require such credentials.
- The **Authentication Type** field on the login page has a value other than Local, such as RSA or RADIUS. As a result, specify which authentication domain to use.
- You are prompted to accept an organizational license.

**NOTE**

When a user with an Active Directory account attempts to log in following expiration or temporary replacement of a password, the **My Info** page appears. On this page, the user must change the password. The password is propagated to update to Active Directory.

**Access the PAM UI Using the PAM Client**

**Follow these steps to use the PAM Client:**

1. On a local workstation where you plan to use the PAM Client, open a web browser, and enter the URL of a PAM server
2. Download the PAM client installer executable.
3. Run the installer.
4. After the installation is complete, launch the PAM Client application and log in.

**NOTE**

For comprehensive information about installing and using the PAM Client, see [Deploy the PAM Client](#).

**Access the PAM UI Using the PAM Access Agent**

**Follow these steps to use the PAM Access Agent:**

1. On a local workstation where you plan to use the PAM Access Agent, open a web browser and enter the URL of a PAM server.
2. Download the PAM client installer executable.
3. Run the installer.
4. After the installation is complete, launch the PAM Access Agent and log in.

**NOTE**

For comprehensive information about installing and using the PAM Access Agent, see [Deploy the PAM Access Agent for Windows](#)

**Password Change on First Login**

When you log in the first time, you are prompted to change your password. Follow these password requirements:

- Differ from the previous password
- Be a length between the Global Settings values for **Min Length** (default: 6) and **Max Length** (default: 14)
- Have at least one (Latin) alphabet character
- Have at least one numerical digit character

## Account Information

You can also specify other account information. To modify these settings, select your account name in the top-right corner of the UI to view and modify your account information. Many of the fields are self-explanatory, but note the following settings.

Basic Info	
RDP Username	Used by the RDP applet as credentials for access to a remote Windows device. This field accepts a name with an embedded backslash to log in to a domain account.
Mainframe Display Name	Display Name that is used by the AS/400 applets TN3270, TN3270SSL, TN5250, TN5250SSL
Keyboard Layout	Conforms the keyboard input to native keyboard output. Select the pull-down arrow to display all available language options.
Administration	
Email self on login	Enables an email to be sent to the email address entered in the Basic Info page. Alerts you when the account is being used by someone else.
Email on Login	Enables an email to be sent to the email address of a specific user or administrator.
Terminal Customization	
SSH and Telnet CLI Terminal Customization	Select this box to display settings for configuring the command-line interface terminal.
RDP Resolution	Select the resolution for the RDP terminal.

## About the Landing Page Displayed After Login

After you log in to the server, the page you see depends on your user role.

- For *standard users* (users who use PAM to access and manage privileged network devices, not administrate PAM), the **Access** page displays. From the **Access** page, you can make connections to target devices and view passwords.
- If you have Global Administrator privileges, the **Dashboard Overview Tab** appears. Users with such privileges include the superuser, the Global Administrator, and the Operational Administrator or Server Control Administrator roles. More information about the **Dashboard** is available [here](#).

### NOTE

PAM also provides the following interfaces for configuring network settings and accessing PAM functionality programmatically:

- Network Interfaces**

PAM provides the following interfaces for configuring network settings on the PAM physical and VMware OVA appliances:

- LCD interface on the front panel of the hardware appliance. For more information, see [Configure Network Connections for the Appliance](#)
- VMware Console for the VMware OVA appliance. For more information, see [Deploy the VMware OVA Template](#).

- APIs**

PAM provides the following APIs for accessing its functionality programmatically.

- [PAM External REST API for Integrating Applications](#)
- [Credential Manager Remote CLI and Java API](#)

## Using PAM

---

The topics in this section describe procedures for *standard users* (end-users who use PAM to access and manage privileged network devices, not PAM administrators).

- [Establish Connection Sessions and View Target Account Passwords](#)
- [Configure Your Account Settings](#)
- [Display and Access Devices](#)
- [Filter Views](#)
- [View and Permit Views of Passwords](#)
- [Set Up Java for Internet Explorer](#)

### Establish Connection Sessions and View Target Account Passwords

The **Access** panel is displayed as the default landing page when a standard user logs in. Users with greater than standard user privileges open the panel by selecting the **Access** entry on the menu bar.

The **Access** panel provides a consolidated interface from which you can:

- Establish a **connection session** to target devices for which you have access permission.
- **View the password** of target accounts (of a target application maintained on a target device) for which you have permission.

#### NOTE

The functionality available on the **Access Devices** panel depends on the platform from which it is accessed. Use the following links to access content that describes the functionality available on the **Access Devices** panel on each platform:

- [PAM Client or a browser that supports applets \(IE 11\)](#): Full functionality
- [Other browsers](#) (for example, Chrome, Edge, Firefox, and Safari: Simplified interface with a subset of functionality
- [Mobile devices](#): Simplified interface with a subset of functionality.

### Review the Access Page

#### NOTE

Mobile users, see [Mobile User Access Page](#).

The **Access** page is available:

- As the unmarked landing page for a standard user
- By selecting the **Access** link on the Menu bar for any user with privileges beyond the Standard User role

The **Access** page provides a consolidated interface from which you can:

- Establish a **connection session** to any permitted Privileged Access Manager Device
- **View the password** of any permitted Target Account (of a Target Application maintained on a Privileged Access Manager Device)

After you log in, a page appears with the the following columns:



- Device Name
- Address
- OS
- Access Methods
- Web Portal
- RDP Applications
- Services
- Target Applications

If your administrator provisioned devices and assigned a policy to you (or your user group), you might have many rows. For example, you might have devices that are named "RH3," "Win2k," "WS2," and more. Each line item corresponds to access features available to you for that device.

For example, an access method named "RDP\_3389" might be available for your download and automatic connection to device "Win2k". Clicking "RDP\_3389" triggers an applet to be downloaded to your computer. The applet automatically executes a connection to the physical device labeled "Win2k". If single sign-on is configured, you might be prompted to enter a user name and password. You might be logged in automatically and land in the home directory.

In the column labeled "Target Applications", a drop-down list corresponds to Device "WS2". There might be a Target Application, such as "MSSQL" on that Device ("WS2"). Indented below that name might be a Target Account ("User1"). The items in this menu prompted Password Views. Thus if you select "User1" you invoke an overlay window that asks for your password viewing credentials. When you supply them, the password appears.

If the number of elements in the drop-down list exceeds thirty (target applications and target accounts combined), a pop-up list appears. The pop-up list shows the complete list of applications and accounts. You can then view the list of target accounts based on your target application. You can also directly search for the target application or the target account.

### **The SSH Access Method Behavior on the Access Page**

The SSH Access Method behavior for autologin using the SSH-2 Certificate Authentication protocol differs from autologin using the SSH-2 Password or SSH-2 Public Key protocols. After configuring the SSH-2 Certificate Authentication protocol, the SSH Access Method applet (MindTerm) connects an SSH Proxy Service in the PAM appliance that performs go-between, actions including SSH-2 certificate authentication. The SSH-2 Password or SSH-2 Public Key protocols do not require this additional layer of processing.

As a result, using the SSH-2 Certificate Authentication protocol reduces the number of simultaneous SSH Access Method applets per PAM Appliance. Additionally, the cryptography settings governing connections to Target Devices via the SSH-2 Certificate Authentication protocol will be configured on the **Configuration, Security, Cryptography** page under the **SSH Proxy** tab, versus the **SSH MindTerm** tab for the SSH-2 Password or SSH-2 Public Key protocols.

## **Use the Limited Functionality Access Devices Panel on Standard Web Browsers**

When you log in to the PAM UI from a standard browser (for example, Chrome, Edge, Firefox, or Safari; *not* Internet Explorer), a limited functionality version of the **Access Devices** panel is available.

The **Access Devices** panel is displayed as the default landing page when a standard user logs in. If you have greater than standard user privileges, select the **Access** entry on the menu bar open the panel.

This limited version of the **Access Devices** panel provides an interface from which you can:

- Obtain the credentials of any target account (of a target application maintained on a Privileged Access Manager device) for which you have privileges in the **Access Devices** table.
- View the details of any credentials that you are using the **Passwords currently in use** table.

The following screen capture shows an example of the limited **Access Devices**

**Symantec Privileged Access Manager**

Super System Info Logout

Dashboard Access Sessions Users Services Devices Credentials Policies Secrets

**Warning:** PAM-CMN-1018: Configuration Password is still the default value.  
PAM-CMN-3356: Remote CA PAM Debugging Services is ON.

(2) Passwords currently in use

Account	Applicati	Host	Device	Auto Contr	Timeou	Reques	Approve	Request Start Date	Request End Date	Status	Action
check...	app1	1.1.1.1	device1	All		super		2022/11/02 1...	2022/11/02 1...	Chec...	<a href="#">Check In</a>
dual...	app1	1.1.1.1	device1	All	10	super		2022/11/02 1...	2022/11/02 1...	Pending	

**Access Devices**

Column: Value: Filter Reset Add Filter My Views

Device Name	Address	Operating System	Target Applications
apikey.xceedium.com	apikey.xceedium.com	Other	Select
device1	1.1.1.1	Other	Select
JITDevice	10.17.41.105	Other	Select

### View the Credentials of Target Accounts for Which You Have Privileges

The **Access Devices** table lists the following information about target applications for which you have permission to obtain the login credentials:

- **Device Name**
- **Address**
- **Operating System**
- **Target Applications**

If your administrator has provisioned multiple devices and has assigned a policy to you (or your User Group), the **Access Devices** table has a corresponding row for each device. For example, you might have devices that are named "RH3", "Win2k", and "WS2". Each line item corresponds to access features available to you for that device.

In the Target Applications column, a drop-down list corresponds to Device "WS2". There might be a Target Application such as "MSSQL" on that Device ("WS2"). Indented below that name might be a Target Account ("User1"). The items in this menu prompt Password Views. If you select "User1", the **Show Credential** page appears.

### View the Details of Credentials That You Are Using

Select the **Password View Requests** to view the details of any credentials that you are using and, optionally, check them in.

**NOTE**

The **Passwords currently in use** table only appears (above the **Access Devices** table) if you are using at least one set of credentials.

**TIP**

To access the fully functional **Access Devices** panel from which you can establish connection sessions to permitted Privileged Access Manager devices, open the PAM UI using the PAM Client or Internet Explorer.

## Use the Access Devices Panel from a Mobile Device

When you log in to the PAM UI from a mobile device, a limited functionality version of the **Access Devices** panel is available.

The **Access Devices** panel is displayed as the default landing page when a standard user logs in. If you have greater than standard user privileges, select the **Access** entry on the menu bar to open the panel.

This mobile version of the **Access Devices** panel provides an interface from which you can:

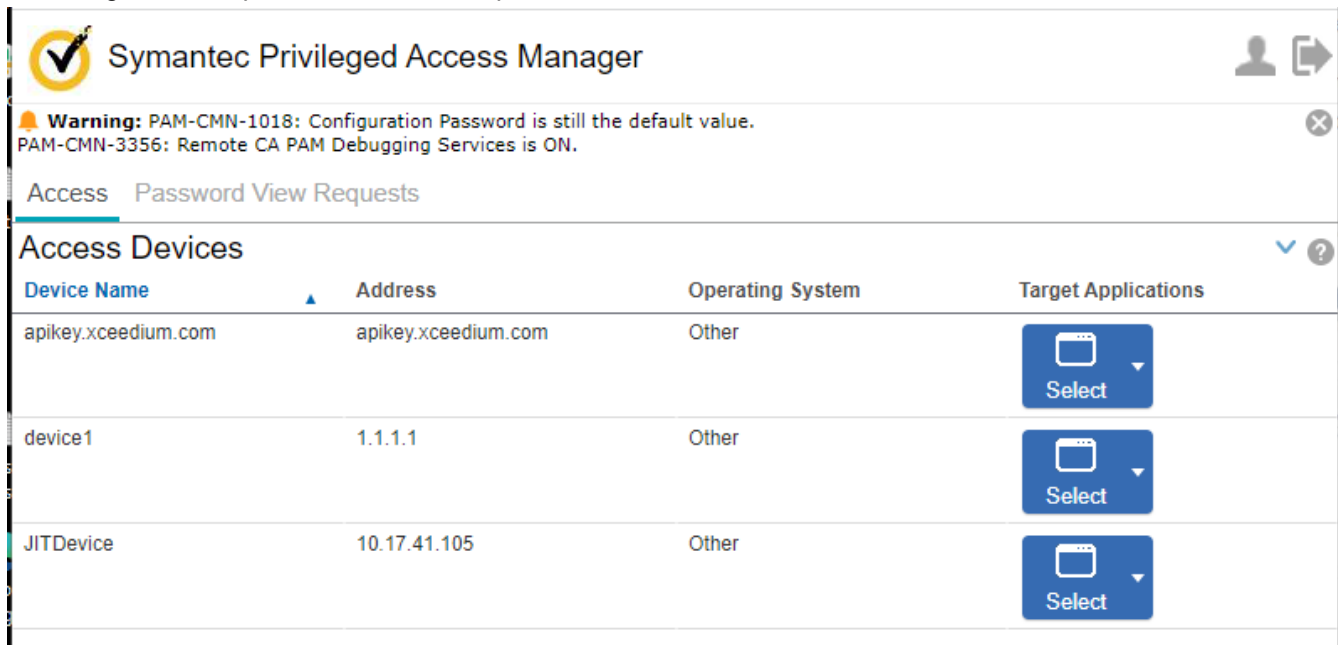
- View the credentials of any target account (of a target application maintained on a PAM device) for which you have privileges.
- View the details of any credentials that you are using.

### View the Credentials of Target Accounts for Which You Have Privileges

Select the **Access** tab to view the **Access Devices** table that lists the following information about target applications for which you have permission to obtain the login credentials:

- **Device Name**
- **Address**
- **Operating System**
- **Target Applications**

The following screen capture shows an example of the **Access**



The screenshot shows the Symantec Privileged Access Manager mobile interface. At the top, there is a header with the Symantec logo and the text "Symantec Privileged Access Manager". Below the header, there is a warning message: "Warning: PAM-CMN-1018: Configuration Password is still the default value. PAM-CMN-3356: Remote CA PAM Debugging Services is ON." Below the warning, there are two tabs: "Access" (selected) and "Password View Requests". The main content area is titled "Access Devices" and contains a table with the following columns: "Device Name", "Address", "Operating System", and "Target Applications". The table lists three devices: "apikey.xceedium.com", "device1", and "JITDevice". Each device row has a "Select" button in the "Target Applications" column.

Device Name	Address	Operating System	Target Applications
apikey.xceedium.com	apikey.xceedium.com	Other	Select
device1	1.1.1.1	Other	Select
JITDevice	10.17.41.105	Other	Select

tab.

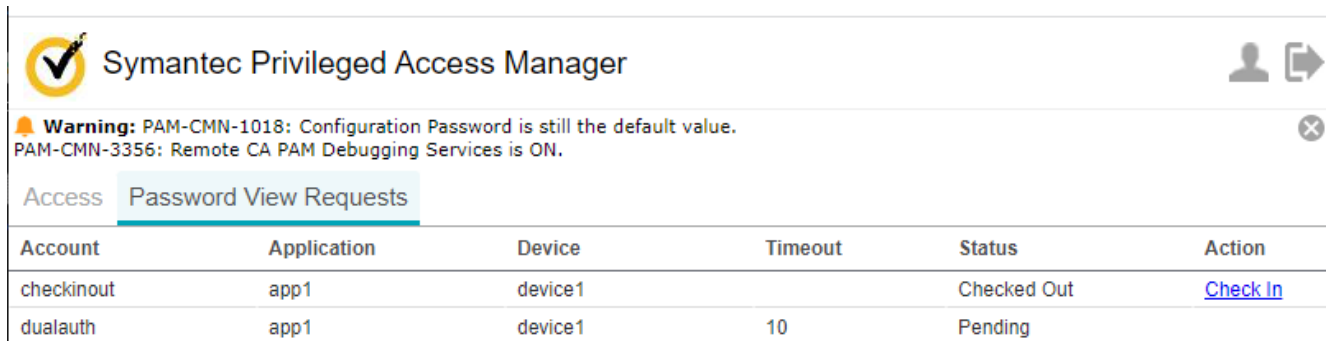
If your administrator has provisioned multiple devices and has assigned a policy to you (or your User Group), the **Access Devices** table has a corresponding row for each device. For example, you might have devices that are named "RH3", "Win2k", and "WS2". Each line item corresponds to access features available to you for that device.

In the Target Applications column, a drop-down list corresponds to Device "WS2". There might be a Target Application such as "MSSQL" on that Device ("WS2"). Indented below that name might be a Target Account ("User1"). The items in this menu prompt Password Views. If you select "User1", the **Show Credential** page appears.

### View the Details of Credentials That You Are Using

Select the **Password View Requests** tab to view the details of any credentials that you are using and, optionally, check them in.

The following screen capture shows an example of the **Password View Requests**



Account	Application	Device	Timeout	Status	Action
checkout	app1	device1		Checked Out	<a href="#">Check In</a>
dualauth	app1	device1	10	Pending	

tab.

#### NOTE

See also [Update Mobile User Password](#)

## Configure Your Account Settings

The first time that you log in, you are prompted to add or edit your name and email and to change your password. To update the information in the **User Information** panel later, select your name in the upper right of the page.

#### NOTE

Mobile users, see [Update Mobile User Password](#).

### Basic Info Tab

Use the following fields to configure basic account information:

#### NOTE

The **Mainframe Display Name** and **RDP User Name** options that were previously on this tab are now available on the [Extended Identities](#) tab.

- **User Name** cannot be edited.
- **First Name**, **Last Name**, and **Email** are required.
- Use **Old Password**, **New Password**, and **Confirm Password** to change your password.
- **Phone** and **Cell Phone** are optional.
- Select one of the following options from the **Keyboard Layout** drop-down list to specify your keyboard language.

#### NOTE

On Windows clients, you can leave the default **Auto** option to use the Windows OS setting for the virtual RDP keyboard. To use a different language for the virtual RDP keyboard, select that language from the list.

For any OS, select one of the following specific-language options:

- **DA** – Danish
- **DA-DK** – Danish (Denmark)
- **DE** – German
- **EN-GB** – English (UK)
- **EN-US** – English (US)
- **ES** – Spanish (Spain)
- **ES-419** – Spanish (Latin America)
- **FI** – Finnish
- **FR** – French
- **FR-BE** – French (Belgium)
- **FR-CA** – French (Canadian)
- **FR-CH** – French (Switzerland)
- **HU** – Hungarian
- **IT** – Italian
- **IW-IL** – Hebrew
- **JA-JP** – Japanese (Japan)
- **NO** – Norwegian
- **PL** – Polish
- **PT-BR** – Portuguese (Brazil)
- **PT-PT** – Portuguese (Portugal)
- **RU** – Russian
- **SV** – Swedish (International)
- **SV-SE** – Swedish (Sweden)

### **Administration Tab**

(Optional) Set the **Email Self on Login** option on the **Administration** tab to configure PAM to send you an email to each time that you log in.

### **Extended Identities Tab**

Configure alternate accounts to access RDP applets, mainframe applets, and Azure SQL Managed Instances on the **Extended Identities** tab.

To specify an alternate account, enter it in the corresponding **Value** field:

#### **NOTE**

The extended identities controls are not enabled until you log in with new credentials after a login session when you are *required* to change your password. That is, they are disabled the first time that you log in to an account and when you log in to make a required password change.

- **RPD User Name:** Enter an account name for use by the RDP Applet or the MSSQL JIT target connector.
- **Mainframe Display Name:** Specify an account name to use to access the AS/400 applets (TN5250 and TN5250SSL).
- **Azure Username:** Specify a valid Azure AD account name (an email address) to use to access an Azure SQL Managed Instance. The specified value must be an account that exists in Azure AD.

### **Terminal Customization Tab**

Use the controls on the **Terminal Customization** tab to customize settings for SSH, Telnet CLI, and RDP terminal settings.

To customize settings for SSH and Telnet CLI terminal sessions, set the **SSH and Telnet CLI Terminal Customization** option. Use the controls that appear to change font, color, character encoding, terminal dimensions, buffer, and scroll position.

To specify the default resolution for RDP terminal sessions, select an option from the **RDP Resolution** drop-down list.  
**Range:** 800 x 600 to Full Screen **Default:** 1024x768

## Preferences

Use the controls on the **Preferences** tab to optionally set the following options.

- Use the following options to optionally override the default date and time display preferences:

- Select a **Time Zone Region**, then a **Time Zone**.
- Select a **Date Format**, such as MM/DD/YYYY.
- Select a **Time Format**, such as 12 or 24 Hour.

### NOTE

The **Server Time** is always displayed in UTC. If you save any changes, they are reflected in the **User's Current Time**. Modifications do not take effect until the next login session.

- Set the **Enable Charts** option to enable graphical charts in the [Credential Manager Activities](#) reports.
- Set the **Application Color Scheme** option to override the global setting and specify whether to display the PAM UI in **Light** (the default) or **Dark** mode:

### NOTE

Dark mode is also not available on the PAM Agent or for all elements and components on other PAM UI platforms, including the following:

- PAM access methods (for example, RDP, SSH, and TELNET) launched from the **Access** page
- PAM LDAP Browser
- Session Recording Viewer
- Threat Analytics
- PAM Report output
- External API Documentation
- Online help
- Alternate Configuration Utility

## Update Mobile User Password

This topic only applies to users who log in from a mobile device.

The first time that you log in, you are prompted to change your password. **User Name** cannot be edited.

To update your password in the User Information window later, follow these steps:

- Select the User icon in the upper right of the Access page.
- Enter your current password in the **Old Password** field.
- Enter a new password in the **New Password** field and the **Confirm Password** field.
- Select **OK** to change your password.

### NOTE

See also [Mobile User Access Page](#).

## Display and Access Devices

Privileged Access Manager can identify and provide connections and passwords to remote devices, applications, and accounts to work on that device. An administrator role involves any type of management of the appliance and its managed objects. This page reviews end-user functions and provides additional information for the administrator.

### List the Devices Available

Your access policy, determining what Devices and passwords you can access, is dynamically applied during your login. This process results in the set of objects available on your Access page.

### Display Settings

To reset your graphical session (RDP, VNC) window size, select the **Display Settings** link to show a pop-up menu with the available size options (pixel width by height - for example, "1024x768"). The currently active option is marked in **bold**.

### Restart Session

Selecting **Restart Session** resets your session to your initial login state, without logging you out.

#### **WARNING**

Product behavior when restarting RDP Application sessions has changed in release 3.2.2. Previously, when you selected **Restart Session** on the **Access** page, the RDP Application applet remained connected to the target device and you could continue using it. Now when you restart a session, the RDP Application applet connection terminates and you must relaunch it to continue. Save your work before restarting a session!

### Filter Views

By default, you see an unfiltered view that shows all Devices and methods that you are permitted to use. You can filter this list by specifying the necessary field values so that it shows fewer Devices. See [Filter Views](#) for more information.

### Access the Devices

#### **WARNING**

**For users without a local account in Privileged Access Manager** (for example, if LDAP or RADIUS provisioned): On your first login, you might be required to go to the **User Information** page if you are not a local User. You then select **Save** before attempting to access a device. This step is necessary to propagate functionally required settings.

To access a device from its line-item listing, select a link on the Access list:

- **Access Methods** (VNC, Telnet, SSH, RDP), **Web Portals**, and your custom **Services** are launched by clicking their blue, named text buttons.
- **Applications** and Privileged Access Manager-defined **Services** appear in drop-down list.

When you hover your mouse over a Service or Web Portal, a pop-up hint window displays target address, port, and other information.

### **Access Method**

Selecting an Access Method downloads to your computer a Java applet customized to use the protocol (RDP, SSH, other). The applet has been specified to initiate a connection to the specified Device automatically.

To launch an Access Method:

From the list or drop-down list, select the desired Access Method button.

### **CLI Applet (Telnet, SSH)**

- If you have selected a CLI-based applet, a MindTerm terminal emulation applet with a control menu appears. **Note:** The MindTerm applet command line window has a 512-column by 512-row limit.
- If you have an SSO (single sign-on) configured (through **Policy, Manage Passwords**), they are applied and the prompt lands logged in.

You can configure terminal window characteristics (window size, font, colors, and other features) at several levels. Verify them with your Privileged Access Manager administrator:

- By an administrator using global default settings
- By an administrator using default settings for a specific Device
- By you for your specific use (overriding the Global Settings) in: **User Information, Terminal Customization, SSH and Telnet CLI Terminal Customization.**

### **SSH with X11 Forwarding**

For an SSH Access Method applet configured to forward X11:

1. From the Access page, launch the SSH applet.  
You are prompted for your **local** display coordinates (default is 0,0).
2. Enter your display coordinates.  
Your SSH session begins.
3. Invoke an xterm for a graphical application. If you are using **Cygwin**, use the "**x-terminal-emulator**" command (not "xterm").
4. You can now start X-Windows commands from the SSH applet.  
The session is then forwarded through the SSH tunnel to the X11 server running on the client host, and graphically displayed to the user.  
For example, using Cygwin:  
From within the SSH applet, invoke: xeyes  
The xeyes now displays on the users local X11 server.

See the settings table in Provisioning: Devices: Set up Devices: Create/Edit Devices for administrator setup of X11 forwarding.

### **Graphical Applet (RDP, VNC)**

Several seconds after you mouse over the applet link, you can select the applet window resolution. You can also select any of your local drives for mapping onto the RDP target.

If you select an RDP applet:

- The applet first displays a splash screen.
- Then, the interface emulation window of the applet appears.  
If credentials are not being passed (for example, through a single sign-on (SSO) configuration), you land at a credentials prompt. You can use the emulated interface as you would with native RDP – in other words, similar to as you would use your server locally.

### **Web Portal**

Selecting a Web Portal invokes a browser session on your computer with the web server on the specified Device. To focus interaction within the Web Portal, the browser controls (File menu bar, Back/Forward buttons, and others) are mostly disabled.

To launch a Web Portal:

- From the list, select the desired portal name.
- If credentials have been configured, they appear (in clear text) in the upper left. You can copy and paste them to fields in the portal interface.
- A new browser window or tab opens and attempts to land at the target website.

### **RDP Application**



Selecting an RDP Application connects to the specified Device and launches the specified RDP Application on the target device.

### **Notes**

- The connection method is either an Access Method or a Service; it is not identified on the Access page. (See the method descriptions elsewhere in this section.)
- If credentials are needed but not passed, connection progress stops at the credentials prompt.

To launch an RDP Application:

1. From the list or drop-down list, select the desired drop-down application name.  
The (hidden) connection method that is specified for this application is invoked.
2. Upon connection and credentials verification, the RDP Application is launched automatically.

### **Service**

Selecting a Service first creates a secure tunnel to the associated Device. This Service then invokes on your computer a communication application that automatically connects to the specified Device. The local path and executable file for the communication application is specified in advance by the Privileged Access Manager administrator. However, you can revise but them using the following procedure:

#### **NOTE**

Do not confuse the following terms:

- a *Service application* that is resident on a client computer
- an *RDP Application* that is resident on a Device
- a [*Target*] *Application* that is used with Credential Manager.

The first group of services is located in the Service column. The second group is in the RDP Application column. The third group is in the Target Application column.

To launch a Service:

1. From the list or drop-down list, select the desired Service button or drop-down selection.
2. The Service application is launched and a connection is attempted using this service.  
**Note:** If credentials are needed but not passed, connection progress waits at the credentials prompt.
3. Simultaneously, a pop-up acknowledgment window appears over the Access page.  
No interaction with this pop-up window is required to execute the Service using the default path.  
The Service name is not mentioned – only the device address and port are.

### **Change Service Local Path to Application**

Following the launch of a Service as described in the previous section, you can change the local path to the application.

If the specified local path to the application does not match the user setting for it, then from the acknowledgment pop-up window the user can:

1. Select Set or change local application to reset the path.  
The pop-up window expands to allow the user to create or revise the local **Path to Application**. This path is initially a copy of the Privileged Access Manager-stored path to the application.
2. Enter the actual path and application executable to be used, and select **Save**.  
This local path will then be substituted for the Privileged Access Manager-stored path the *next* time that you launch this Service.

## Filter Views

Pages in the PAM UI that have lists can be filtered, and those filters can be saved as Views. The Access page, Sessions, Users, Devices, Accounts, and so on, can all be filtered. You can add multiple filters, and can save them as a View, and can make a View the default View. The Reset button displays an Unfiltered list, or View. You can hide the Filter controls by clicking the "up" arrow to the right of the page heading, next to the Help question mark icon.

### Filter a List and Save a View

Every page with a list of objects or records has a row of filter controls above the list.

To filter a list, follow these steps:

1. Select a **Column** to filter on.
2. Enter a **Value**. Most columns accept free text. Some columns with a limited set of values, such as Operating System or Application Type, present a drop-down list or dialog for selection.

#### **NOTE**

Columns with limited values that are presented in a dialog allow multiple selections. For most columns, the filters treat these selections with "OR" logic. These column filters, such as Location, Operating System, and Device Type, display data for objects meeting any of the options that you select. However, the Tag column filter, available on the Access or Manage Devices pages, uses "AND" logic. Unlike unique attributes such as Operating System, a Device can possess multiple Tags. For example, if you filter on the Tag values of "AD" and "LDAP", you return only Devices possessing both tags, rather than Devices possessing either or both.

3. Select **Filter** to see the results.
4. To filter on multiple columns, select **Add Filter** and repeat the previous steps for each column you want to filter on. Select the **X** to remove a filter.
5. To undo the filter and restore the original unfiltered list, select **Reset**.
6. To save the filter results as a permanently stored View, select **My Views**, then **Save As**. The **Save As** window appears.
7. Enter a **Name**. Select **Set as Default View** if you want the view to appear whenever you view this page.
8. The **Columns** tab allows you to remove or add existing columns to the list display.
9. Select **OK** to save.  
The View can now be invoked from **My Views**. You can edit existing views from **My Views**, **Manage Views**.

### Text Filter Details

#### **Filtering on One or Two Characters**

If you filter a page list using a value of only one or two characters, the results return only entries that *start with* those characters. Characters can be single-byte, like English or multi-byte, like Japanese. The results do not include entries that *contain* those characters only in other parts of the string.

This behavior does not apply to Credentials page lists.

For example, if you filter on the Name column and you specify the characters "ca " the resulting list shows `capam` but not `tap.ca.com`.

#### **String Comparison**

The filter uses MySQL-style string comparison functions:

`%` matches any number of characters, including zero characters.

`_` matches exactly one character.

#### **Escape characters**

To filter on an otherwise reserved character, use "\" as the escape character. For example:

\% matches one "%" character.

\\_ matches one "\_" character.

\\ matches "\"

The final example could be used to filter on the File Path or Execution Path column of the A2A Scripts list.

## View and Permit Views of Passwords

### View a Password

Active Target Applications and their associated Target Accounts are listed on the Access Page. Every Target Application that is associated with a Device is identified in the drop-down list in the Target Applications column. Every Target Account that is associated with each application appears in a nested list. After selecting a Target Account from the drop-down list for a Device, a pop-up View Account Password Request window appears. After entering the Password (for the currently logged-in Privileged Access Manager user), the credentials are displayed in the pop-up.

### View a Password Requiring Dual Authorization

Dual Authorization requires access to the Credential Manager menu using the FirecallUser role. The menu is not available to a Standard User from the Access page.

### Check in a Password

You can monitor check-out status and can perform check-in from the Access page. If another administrator attempted to view this password, the message "This account is checked out by another user" appears in place of the View Account Password pop-up. For the second administrator to view (and also check out) the password, the first administrator clicks the **Check In** link for that account. The first administrator does not need to switch to the **Credentials Manager Target Accounts** panel.

## Set Up Java for Internet Explorer

The only browser Privileged Access Manager supports is Microsoft Internet Explorer 11. IE 11 is the only browser that still supports NPAPI, which RDP and SSH access Java applets use. If you use IE11, install the latest Java 8 version on the desktop. Ensure that Internet Explorer and Java are using the same 32-bit or 64-bit version. The 32-bit version of IE is used by default regardless of whether the Windows OS is 32-bit or 64-bit.

### Internet Explorer Version

You might not know which version of Internet Explorer 11 you are running. Regardless of whether Windows is running a 32-bit or 64-bit operating system, Internet Explorer is probably running a 32-bit version, which is the default. To determine which IE version you are using, follow these steps:

1. Open Internet Explorer 11.
2. Select the **Tools** gear icon.
3. Select **About Internet Explorer**.  
If the About window contains "64-bit Edition", then you are using the 64-bit version. Otherwise, it is 32-bit.
4. **Close** the About window.
5. To see if Java is enabled in Internet Explorer, select **Tools, Manage add-ons**. If the Add-ons chart shows a Java row, the Architecture column shows "32-bit", "64-bit", or "32-bit and 64-bit". If IE is 32-bit and the Add-ons window shows "32-bit" or "32-bit and 64-bit", it should work with PAM.

## Java Version

If you have installed Java on your computer, determine the version. Follow these steps:

1. In Windows, select **Settings**, then search for Control Panel.  
The All Control Panels window appears.
2. Select **Java**.  
The Java Control Panel appears.
3. Select the Java tab, then the **View** button.  
For each Java version, a row appears with an **Architecture** column. "x86" denotes 32-bit while "x86\_64" denotes 64-bit.  
The **Platform** column should show 1.8 or greater. If not, upgrade Java.  
The **Enabled** column should be checked.

If your IE and Java architectures match, the browser should work with PAM.

## Version Compatibility

If Internet Explorer and Java are not working together, you receive a dialog when you connect to Privileged Access Manager. The message states "The page you are viewing uses Java. More information about Java support is available from the Microsoft website." The solution is probably to install Java for the appropriate 32-bit or 64-bit architecture. If you install a new version of Java, you should close and open Internet Explorer before trying to use it.

See the Java website for more information about plug-in installation: [https://java.com/en/download/faq/java\\_win64bit.xml](https://java.com/en/download/faq/java_win64bit.xml)

For more information about further troubleshooting Java and Internet Explorer, see [https://www.java.com/en/download/help/ie\\_tips.xml](https://www.java.com/en/download/help/ie_tips.xml).

### NOTE

For instructions on downloading, installing, and using the PAM Client, see [Deploy the CA PAM Client](#).

---

## Configuring a PAM Server

---

Before you can use a PAM server, you must configure many required and optional configuration settings.

Appliance access and licensing settings depend on your appliance platform:

- **Hardware:** A pre-licensed physical appliance. For configuration information, see [Deploy the Hardware Appliance](#).
- **VMware OVA:** Provided by your account representative with a link to download the OVA to your vCenter location so that you can create a VM. You also receive a license to activate the instance.
- **AWS AMI:** Provided by your account representative with permission and an AMI number so that you can create an instance within your AWS account. You also receive a license to activate the instance.
- **Azure VHD:** Provided by your account representative with a link to download the VHD to your Azure location so that you can create a VM. You also receive a license to activate the instance.

Network context configuration:

- **Hardware:** Use the LCD display on the left side of the front panel of the appliance. See [Configure Network Connections for the Appliance](#).
- **VMware VM:** After you power on your VM, use the VMware Console to access the same controls as are provided by the LCD on a hardware device.

### NOTE

For clustered implementations, the blue globe icon on the title of a configuration panel signifies that the configuration is replicated to all cluster members. Configure changes to settings with the blue globe icon on the *primary* site of your cluster; they are not configurable on *secondary* sites.

### Required Configuration Settings

- [Date/Time](#) – Set up your appliance to synchronize with NTP time servers
- [Licensing](#) – Your appliance must be licensed for target Devices and feature use
- [Security](#) – Provide a certificate; optionally, set up PKI/CAC, specify CRL, sign applets, activate SAML use, activate API access

### Optional Configuration Settings

- Third Party – Configuration connection to these optional network resources:

- [AWS API Proxy](#)
- [VMware](#)
- [Vmware NSX API Proxy](#)
- [LDAP, RADIUS, or TACACS+](#), and [RSA](#) for [user authentication](#)
- [SafeNet or Entrust Hardware Security Modules](#) for Credential Management
- [Microsoft Office 365](#)
- [Splunk](#)
- [Network](#) – extra network interfaces as needed
- [Logs](#) – Configure log and session recording output to external storage
- [trap server](#)
- [Clustering](#)
- [Configuration and Database Backups](#)
- [Diagnostics and Troubleshooting](#)
- [Email Setup for Monitoring](#)
- [Power, Reboot, and FIPS Mode Controls](#)
- [Set Your Locale](#)
- [Master Provisioning Settings](#)

## Configure Global Settings

Use the **Global Settings** panel to set universal options for all users and devices.

### NOTE

Credential Manager-specific settings are configured in a separate location. See [Set Up Credential Manager Operation Settings](#) for more information.

Use the controls on the **Settings, Global Settings** panel to set universal options that apply for all users and devices. The controls are presented in the following tabs.

- [Basic Settings](#)
- [Passwords](#)
- [Accounts](#)
- [Alerts](#)
- [Applet Customization](#)
- [Client Settings](#)
- [SAML](#)
- [Threat Analytics](#)
- [Default Preferences](#)
- [Secrets Management](#)

To commit any settings changes that you make, select the **Save** button at the bottom of the panel. The screen refreshes to display the updated configuration and the "Global Settings Saved" text appears on the screen.

### **Basic Settings**

The basic settings include:

- **Default Auth Method** (Login Page): Specify the default authentication method that appears on the login page from the following values. At least one user must be created with that authentication method before this option becomes available. The options are:

- Local
- LDAP
- RSA
- RADIUS
- TACACS+
- PKI-CAC
- LDAP+RSA
- LDAP+RADIUS
- **Default Page Size:** Specifies the number of Device line items visible when a user initially hits the **Access** page after login.
- **Login Timeout:** Specifies the number of minutes of inactivity between a PAM user and the PAM UI (including connections to targets) before their session times out. This value is automatically extended when an active connection to a target device exists. The default value is 10. The maximum value is 2880 minutes (48 hours).
- **Connection Idle Timeout** (formerly **Applet Timeout**): Specifies the default number of minutes of inactivity before a connection (such as Telnet, SSH, Virtual Machine) with an external device times out. Users assigned policies with the [Extended Timeout](#) option enabled can override this value. The **Connection Idle Timeout** value cannot exceed the value of the **Maximum Connection Idle Timeout** setting.
- **Maximum Connection Idle Timeout:** Specifies the maximum **Connection Idle Timeout** value that a user can specify when initiating a connection with most external devices. The following device types do not support **Maximum Connection Idle Timeout**:
  - RDP Proxy Service
  - Web Portals
  - VNC devices

The absolute maximum value is 2880 minutes (48 hours).

#### NOTE

Verify that the **Maximum Connection Idle Timeout** value is long enough to accommodate the longest job that a user might run.

- **Table Refresh Interval:** Specifies the default refresh interval, in seconds, for the tables displayed in the following locations:
  - **Access** (from a browser other than Internet Explorer): **Passwords Currently In Use**
  - **Devices, Discovery:**
    - **Device Scan History** tab
    - **Discovery Jobs** tab
  - **Credentials, Discovery:**
    - **Scan Profile History** tab
    - **Discovered Accounts** tab
  - **Credentials, Manage Targets, Accounts**
  - **Credentials, Workflow, My Password View Requests**
  - **Credentials, Workflow, My Password View Approvals**
  - **Credentials, Workflow, All Password View Requests**
  - **Devices, Socket Filter Agent**
  - **Management Console: Staging Task Events**

The default interval is 60 seconds, the minimum interval is 30 seconds, and the maximum interval is 3600 seconds
- **Scan Purge Interval:** Specifies the number of days to keep Discovery scans.
- **Default Device Type:** Define the default template that is provided when a Device is added manually. The choices can be overridden on the template itself.

- **Access:** Default: Initially active and selected
- **Password Management:** Checkbox is active only with a Password Management license.
- **A2A:** Checkbox is active only with an A2A license.
- **External API Buttons**
  - **Enable:** Show and activate the **Try It Out** test button at the bottom of every API page in the **API Doc**. The **Try it Out** button enables external API calls from that page. This option is activated by default, but the Enable External REST API option in **Configuration, Security, Access** is not.  
To prevent external API calls from that page, clear the **Enable** checkbox for the Enable API Buttons setting.
- **Allow Bulk Network Scan:** When enabled, an Administrator can run a bulk scan of the network (Host/Port) to determine the status of ports (open/filtered). For information about how to run a Bulk Network Scan, see [Tools](#).

## **Passwords**

You can customize the password requirements for **Local** users by changing these fields. Other authentication method password policies are enforced by their infrastructure and PAM cannot control them. Unlike other accounts, the *super* account never expires. *Super* is not deactivated, even if the password failure limit is activated.

- **Security Level:** Specifies the level of password security that you require for User passwords:
  - **0 - New Password:** The new password must be different from the previous password.
  - **1 - 0+ Length Constraints:** Level 0 and password length must be between the Minimum Password Length and the Maximum Password Length, which are defined on this page
  - **2 - 1+ Require [a-zA-Z0-9]:** Level 0, 1 and password must have both an alphabet character and a digit.
  - **3 - 2+ Both Upper and Lower Case:** Level 0, 1, 2 and password must have both an Upper and Lower alphabet character.
  - **4 - 3+ Special Character:** Level 0, 1, 2, 3 and password must contain a special character such as: !, @, #, \$, %, ^
  - **5 - DoD strong password:** DoD requires a minimum of 15 characters. There must be *at least*:
    - Two uppercase letters
    - Two lowercase letters
    - Two integers
    - Two special characters, such as: !, @, #
- **Minimum Length:** If the Password Level is 1 or above, set the minimum password length.
- **Maximum Length:** If the Password Level is 1 or above, set the maximum password length.
- **Change Interval (Days):** Specifies the number of days between forced password changes for all users.
- **History:** Specifies the number of recent passwords that cannot be reused.
- **Failure Limit:** Specifies the number of failed login attempts before a user account is deactivated.
- **Failure Counter Reset (Minutes):** Specifies the number of minutes for which an account is deactivated after exceeding the **Failure Limit**.

## **Accounts**

- **Disable Inactive After (Days):** Specifies the number of days after which inactive user accounts are disabled. If the backup is older than the time limit, accounts are disabled when restoring a database from a backup.
- **Remove Disabled After (Days):** Specifies the number of days from when an account is disabled until it is deleted.
- **Forced Deactivation Alert:** Select an administrator to receive an alert when a user is deactivated. Monitoring must be configured for this feature to function. See [Set Up Email for Monitoring \(Legacy\)](#) for more information.
- **Email Deactivation Reminder:** Determines when to send an email to inactive users to remind them before their account gets deactivated. This option also specifies the subject line and body text for the email that is sent to users.



- **Remind Before Deactivation (Days):** Specifies the number of days when to send an email reminder to inactive users before their account gets deactivated.
- **Email Subject for Reminder:** Enter the text for the subject heading of the reminder email.
- **Email Body for Reminder:** Enter the body text for the reminder email.
- **Email After Deactivation:** Determines the subject line and body text for the email that is sent to users whose accounts have been deactivated due to inactivity.
  - **Email Subject for Deactivation:** Enter the text for the deactivation notice in the subject heading of the email.
  - **Email Body for Deactivation:** Enter the body text for the deactivation email.

**NOTE**

The Deactivation task runs every day at 2 AM, UTC time. The Deactivation reminder task runs every day at 2:15 AM, UTC time

The email reminder and deactivation email notifications require you to configure the SMTP email server. See the [Configure the Email Server](#) section the UI in the [Configure Email Preferences for Password View Policies](#) topic for more information.

**Alerts**

The options on the **Alerts** tab (formerly titled "Warnings") allow you to configure three optional messages to present to users. They can be customized to reflect individual company policies.

- **Show License Warning:** Set this option to display the specified warning text on the login page for all users. Double-byte characters such as those used for traditional Chinese are supported for warning messages. Select **User must accept license** to require each user to accept the license.

**NOTE**

The License Warning box scrolls to accommodate a long message. Upon setting either option, a text field in which you can customize the warning message appears.

- **Show Recording Warning:** Set this option to display the specified notification when a user opens a recorded applet or service session. For example, when a user opens an SSH console, the following warning appears in the window title bar and in the console: **"Warning you are being monitored."**

**NOTE**

The **Show Recording Warning** option is ignored for *applet* sessions that are made by users who are a member of any user group, deferring to the **Applet Recording Warning** setting specified for the group or groups. This global setting applies for *all* TCP/UDP and RDP service sessions.

**NOTE**

The specified message text is also used for applet recording warnings, even if the **Show Recording Warning** option is not set.

- **Show Informational User Message:** Set this option to display the specified information (for example, notice of planned maintenance) when a user logs in to PAM. For more information, see [Display a Message to Users at Login](#).

**Applet Customization**

The **Applet Customization** tab allows specification of the default terminal display characteristics for all users and all devices. These settings apply for Telnet and SSH applets, and include a switch to allow or disallow copy-and-paste text buffering.

- An administrator can override the defaults on a device basis by changing the **Terminal Type**, **Key Mapping**, and **Terminal Customization** settings for individual devices.
- A user can override the defaults by changing the **SSH and Telnet CLI Terminal Customization** on the **User Information** page.

Clicking the **Configure Terminal Settings** link button brings up a submenu with various terminal settings that you can define on a global basis. These settings are the systemwide default settings. Any terminal customization that is made at the user, user group, device, or device group level takes precedence.

#### NOTE

User terminal customization supersedes device terminal customization, which in turn supersedes global terminal customization.

- **Character Encoding:** *Default:* UTF-8
- **Font Family:** *Default:* Monospaced
- **Font Size:** *Default:* 12
- **Cursor Foreground:** *Default:* #33ff33
- **Foreground Color:** *Default:* #ffffff
- **Background Color:** *Default:* #000000
- **Terminal Size:** *Default:* [80,24]
- **Buffer Size:** *Default:* 100
- **Scroll Position:** *Default:* Left
- **RDP Keyframes Duration:** The keyframe duration determines how RDP is compressed. A small keyframe duration is equivalent to more frequent full frames of video data. The increased frequency results in a large file, but allows more a rapid seek in the RDP viewer. For sessions using RDP 6.1, file size can be reduced significantly by increasing the keyframe duration. Reductions to about half the size have been observed.
  - Small (Fast Seek/Large File): *Default*
  - Medium
  - Large
  - X Large (Slow Seek / Small File)
- **Web Recording Quality:** Specify the color depth and frame rate to use when recording a web portal session:
  - High: 24 BPP / 7 FPS (default)
  - Medium: 16 BPP / 5 FPS
  - Low: 8 bits per pixel / three frames per second
- **Applet Copy Paste:** Enable the use of copy and paste within any applet: This feature activates an Edit menu with Copy and Paste commands. When this option is disabled, the Edit tab is still visible but it is dimmed.
- **RDP Drive Mapping:** Configure RDP drive mapping to provide faster file sharing between the user workstation and the target server. Do the following steps to enable and configure this feature:
  - a. Set the **RDP Drive Mapping** option. A button Appears beside the pin icon in the upper toolbar. Hovering your cursor over the icon displays a tool tip that says "Add new device for mapping"
  - b. Click the **Add new device for mapping** button.
  - c. On the dialog that appears, select a folder on the local system to map to the target server.

#### NOTE

The name of the folder on the local system must only contain ASCII characters (that is, characters in non-English locales are not supported).

- **SSH Terminal File Transfer:** When "Enable SCP/SFTP" is selected, the MindTerm based SSH Access Method applet provides the menu items "**Plugins, SFTP File Transfer**" and "**Plugins, SCP File Transfer**". Each menu item invokes a new applet window to operate SFTP or SCP, which provides a file transfer interface. See [Display and Access Devices](#) for details on the controls.
- **Transparent Login Cache:** After using the Learn Tool and testing transparent login configurations, you can enable the Transparent Login Cache. This feature caches the Learn Tool, the Transparent Login Agent, and the Control Viewer on the RDP server. On subsequent connections to that Windows target, the load times for these applications are reduced.
- **Retrieve Public Address:** An administrator can enable or disable the Java applet Access Agent to retrieve the public address of the user. After a user logs in to PAM, the Java Applet Access Agent is downloaded to the user desktop. The applet retrieves the address of the gateway that is used for external access for auditing and for the VMware NSX

feature. In some environments, this behavior is not desirable. The Retrieve Public Address setting lets administrators disable this feature.

## **Client Settings**

Use these settings to control the distribution and use of the PAM Client.

- **Operating Mode:** Select **Enabled** to allow PAM Clients to log in to this appliance.
  - **Distribution Method:** Select one of the following options:
    - **Internet (Content Delivery Network)** : Allow PAM to engage a PAM to deliver client installers (following requests from the PAM UI login page).
    - **Intranet:** Use the CDN conforming server that you specify in the **Intranet Server** field to deliver installers
- NOTE**  
For more information, see [Use a Private Content Delivery Network to Distribute the Client Installer](#).
- **Download Button on Login Page:** Select **Enabled** to display and activate the **Download PAM Client** buttons. These buttons appear below the white panel on the login page.

## **SAML**

Use these settings to adjust SAML Web SSO authentication.

- **Require Inherited SAML Auth:** Select this option to force the inheritance of the user record **Authentication** setting on all members of a User Group. All group members inherit the settings regardless of whether individual authentication settings are set to "SAML". This setting is selected by default.
- **SAML Re-authentication Period:** Specifies the number of minutes of inactivity before a SAML session times out. The session is between the Service Provider and PAM as an Identity Provider. After a timeout, the next SSO request requires the user to log in again. Default: 60 minutes

## **Threat Analytics**

See the [Threat Analytics documentation](#) for information about the options on the **Threat Analytics** tab.

## **Default Preferences**

You can customize how Privileged Access Manager displays dates and times in the UI. Dates are stored in UTC, but can be displayed in the specified time zone for the user. Selecting a custom time zone can only be done through the GUI. This tab sets default references for all users, while [user information preferences](#) set preferences only for the logged on user.

- Select a **Time Zone Region**, then a **Time Zone**.
- Select a **Date Format**, such as MM/DD/YYYY.
- Select a **Time Format**, such as 12 or 24 Hour.

### **NOTE**

The **Server Time** is always displayed in UTC. If the user saves any changes, they are reflected in the **User's Current Time**. Modifications do not take effect until the next login session.

- **Enable Charts:** Set this option to enable graphical charts in the [Credential Manager Activities](#) reports.
- **Application Color Scheme:** Specify whether to display the PAM UI in **Light** (the default) or **Dark** mode by default. (Once they are logged in, users can change the color scheme in the local [account settings](#).)

### **NOTE**

Dark mode is also not available on the PAM Agent or for all locations on other PAM UI platforms, including the following elements and components:

- PAM access methods (for example, RDP, SSH, and TELNET) launched from the **Access** page
- PAM LDAP Browser
- Session Recording Viewer
- Threat Analytics
- PAM Report output
- External API Documentation
- Online help
- Alternate Configuration Utility

The global **Application Color Scheme** setting also controls the color scheme of the login panel when accessing the PAM UI from a web browser. (This setting cannot be overridden by local account settings.)

### **Secrets Management**

Use the **Maximum Secret Extension (Days)** option to set the maximum number of days that can be specified before secrets are expired or deleted, up to 365 days.

For more information, see [Managing Secrets](#)

## **Configure RDP Proxy Service Settings**

An RDP Proxy Service invokes a local third-party RDP application on a client to connect to a device. Native RDP Client support extends the Access controls to any native RDP client. To create an RDP proxy service, see [Create an RDP Proxy Service to Access a Device](#).

This content describes how to define configuration settings for your RDP Proxy Service.

**To enable and define settings for an RDP Proxy service, follow these steps:**

### **NOTE**

The target server is the server that you connect to using the RDP Proxy.

1. Select **Configuration, RDP Proxy, RDP Proxy Configuration**.
2. Select the following options, as appropriate:
  - Copy and Paste** - Enable copy and paste between the host machine and target server.
  - RDP Drive Mapping** - Enable file transfer between the host machine and the target server.
  - Transparent Login Cache** - After Using the Learn Tool and testing transparent login configurations, you can enable the Transparent Login Cache. This feature caches the Learn Tool, the Transparent Login Agent, and the Control Viewer on the RDP server. On subsequent connections to the Windows target, the load times for these applications are reduced.
  - Log Level** - Select Info or Verbose from the drop-down list. The verbose level provides detailed information about each event.
3. Select **Save** to commit your changes.
4. Optionally, to configure Kerberos Support for your RDP Proxy Service, see [Kerberos Authentication Support in RDP Proxy Service](#).

## **Default Administrator Accounts**

Privileged Access Manager provides two default administrative accounts to manage the product. The "super" account is for Global Administrators, and the "config" account is for configuration administrators. The super account is visible in the Manage Users list, while the configuration account is not.

## **Initial Administrator Login**

All User accounts other than "config" land initially at the **User Information** page, which provides basic User account settings that the user can manage. The user must enter a new password before leaving the page.

## **The Global Administrator (Super) Account**

Privileged Access Manager has a preconfigured global administrator account named **super**. The super account has global access to all configuration privileges for all functionality. The super account cannot be deleted. To change the password from the default, select the user name in the upper right corner. Change the Password in the Basic Info tab. You can change the Administrator login ID from "super" to something else using the [Configuration Utility](#).

When you initially log in to the product, you are logged in as super, with the password "super".

## **The Configuration Manager Account**

Use the configuration account for initial setup. To change the password from the default "config", select the user name in the upper right corner. Change the Password in the Basic Info tab.

Because the username "config" is commonly used, consider also changing the **Login ID** in addition to the **Password** using the **Change Password** page. The Change Password page is only visible from the [Configuration Utility](#).

## **Master Account Security**

After you set up user accounts, you can configure an account for access to the Configuration menu. If a user is granted permission to the Configuration menu, the **Configuration** button appears in the menu bar. When a Configuration menu item is accessed, the current user account credentials are used to log in automatically. Any changes are audited with an individual user ID.

The **Configuration** menu – presented to the configuration professional during initial "config" account access. Use it to configure the appliance before it is provisioned to users and devices.

We recommend that you change the password from its default value after the first logging in. When you log in as "super", you receive a warning message as long as the "config" password remains the default value, "config".

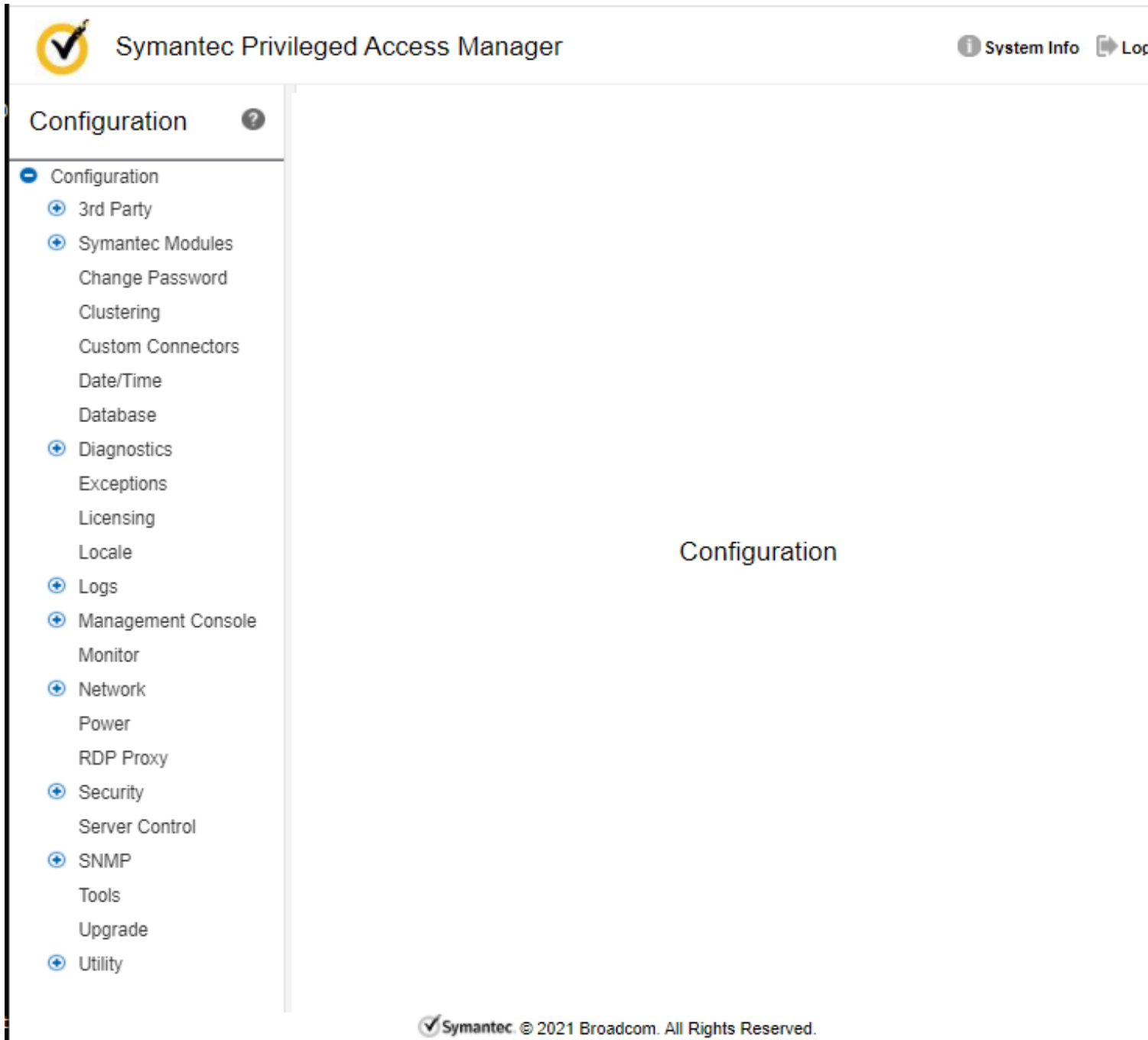
# **Alternate Configuration Utility**

If a bad patch or failed upgrade is applied to PAM, the Tomcat server that launches the regular UI might not start. If this problem occurs, use the Configuration utility. The Configuration utility is an alternate method to manage the configuration and upgrade tasks.

The Configuration utility provides the entire Configuration menu, including upgrade, but no provisioning options.

### **To access the utility:**

1. Open a browser. The Configuration Utility is available only from a browser.
2. Enter the same IP address or host name of the appliance but with **config** appended to the URL. For example:  
`https://11.12.33.123/config/` (IPv4) or `https://[fd6d:8d64:af0c:1:0:242:22:233]/config/` (IPv6)
3. When you are prompted to sign in, enter **config** for the username and password then select **Sign in**.  
The UI opens, displaying only the Configuration menu.



Unlike the standard Configuration menu, the utility has a Change Password option, which lets you:

- Change the login ID and password for the **config** user.
- Change the administrator login name from **super** to something else

For details, see [Change Login for Config or Super User](#).

## Change Login for Config or Super User

The Change Password page is only available in the [Alternate Configuration Utility](#).

### **Change Config User Login ID and Password**

To change the "config" user or password, follow these steps:

1. Log in to the Configuration site.
2. Select **Change Password** on the Configuration menu.
3. Under **Change Config User Login ID and Password**, you can change either the ID or the password or both.  
The replacement ID is still available here, even if it is not "config."
4. Enter a new Login ID if desired.
5. Enter a new password and confirm it.
6. If you change your mind before updating, select **Reset**. The Login ID reverts to its saved value, and the Password and Confirm fields revert to blank.

#### **NOTE**

When you select **Update**, you are logged out and you have to log in with your new "config" ID and password.

7. Select **Update** to save your changes.

### **Change Administrator Login Name**

To change the "super" administrator user name, follow these steps:

1. Log in to the Configuration site.
2. Select **Change Password** on the Configuration menu.  
You can change either the ID or the password or both.  
The replacement ID is still available here, even though it is not "config."
3. Enter a new Login ID.
4. Enter the existing password for "super".  
You need the password for "super" to change its login name.
5. If you change your mind before updating, select **Reset**. The Login ID reverts to its saved value.
6. Select **Update** to save your changes.

**Note:** You can change the password for "super" when logged in as "super" as any User would change their password. Use the User Information page, accessible by clicking the user name ("super") link in the upper right of the UI.

## **Licensing and Product Usage Reporting**

This content describes how to view your current licensed capabilities, install a new license, and configure product usage reporting (telemetry). You access licensing options from the **Licensing** page (**Configuration, Licensing**).

### **View Current License Capabilities**

The Current License tab lists the available capabilities:

- **Access Devices:** Maximum number that you can use
- **Password Devices:** Maximum number that you can use
- **A2A Devices:** Maximum number that you can use
- **Mainframe Capability:** Indicates whether enabled or disabled
- **AWS Capability:** Indicates whether an AWS connection is enabled or disabled
- **AWS API Proxy Users:** Maximum number that can be provisioned
- **VMware NSX API Proxy Users:** Maximum number that can be provisioned
- **VMware Capability:** Indicates whether the connection is enabled or disabled
- **External API Capability:** Indicates whether the API capability is enabled or disabled
- **Office365 Capability:** Specifies whether an Office365 administrative account is enabled or disabled
- **SafeNet HSM Capability:** Indicates whether SafeNet HSM is enabled or disabled. If SafeNet is enabled, Entrust cannot be enabled.
- **Entrust HSM Capability:** Indicates whether Entrust HSM is enabled or disabled. If Entrust is enabled, SafeNet cannot be enabled.
- **PAM Management Console Capability:** Specifies whether this capability is enabled or disabled.
- **SailPoint:** Indicates whether SailPoint is enabled or disabled.
- **Start Date:** Beginning date when the license takes effect.
- **End Date:** Date when your license expires. Applies only for PAM deployed on an AWS AMI instance.
- **Type:** Indicates whether the license is Perpetual (no end date), Temporary, or an Evaluation license. Evaluation licenses are also temporary.

### **Install a New License**

When you obtain a new or an updated license, you must install that license. For virtual machines, instructions for obtaining license files are included with the image download. For each hardware appliance, a license file is prepared by Broadcom and installed with the file.

#### **Follow these steps:**

1. Go to **Configuration, Licensing**.
2. Select the **Install New License** tab.
3. Use **Choose File** to locate the license file on your system. The license file is of type XCDLIC.
4. Select **Upload License File**.  
The **Verify New License** window appears.
5. Verify that the capabilities that are listed are expected and appropriate.
6. Select **Save New License**.

You have to log out and log back in for some options to appear in the interface, such as Entrust or SafeNet HSM.

#### **NOTE**

Licensing no longer detects NIC changes when generating the hardware identification string. This change allows you to add or remove NICs from running instances without breaking the licensing.

### ***Virtual Devices that Exceed License Limits***

A fixed number of device permits for each device type are created with each license. When you add a device rather than import one, a license permit must be available to save that device.

If an imported device exceeds the permit count, the appliance provides a device record, but the device is not provisioned. The device is a placeholder but not operational. The device has no Access or Password Management capability. If you attempt to assign and save the device, the attempt is rejected. When a permit becomes available or another permit is added, you cannot use the device.



## Configure Telemetry to Record Product Usage

Select the **Telemetry Data** tab on the **Licensing** page to enable collection of product usage data. For more information, see [Telemetry Data](#).

### NOTE

If you are licensed to use PAM under a Portfolio License Agreement (PLA) subscription, you must configure PAM to collect and send usage data.

## Configure Network Settings

Configure the network configuration settings for your PAM server on the **Configuration, Network, Network Settings** panel.

The basic network information is shown in the **Gateway** and **Network Interfaces** fields. These fields are the only required settings, except for an AWS AMI instance where a DNS server is the only required setting. If necessary, specify information necessary for DNS routing. For an AMI instance, the DNS setting is provided by the AMI instance and you must enter that value.

### Complete the following fields, as required:

- **Hostname:** Specify a unique hostname for the PAM server. Use this setting to distinguish the servers in a cluster. The IP address is not sufficient.
- **Domain Name:** Specify one or more (space- or tab-delimited) domain names using their top-level and second-level domains (for example: example.com) if you require them for any of the following use cases:
  - To provide the domain name for the mail system (`/etc/mailname`). For more information, see [the mailname man page](#).

### NOTE

Only a single domain name is required for this use case. If multiple domain names are specified, the first listed domain name list is used.

- To create an entry in the `/etc/hosts` file (in the form of `IP HOST.DOMAIN HOST`).

### NOTE

Only a single domain name is required for this use case. If multiple domain names are specified, the first listed domain name list is used.

- To append to unqualified (short) hostnames in DNS queries to create fully qualified hostnames. For example, if a short hostname is "host1" and the specified domain name is "example.com" then the resulting DNS query searches for "host1.example.com."

If multiple domain names are specified, PAM uses them in the specified order until the resulting DNS query returns a valid fully qualified hostname.

### IMPORTANT

Wildcards are not permitted in domain name definitions. Use spaces or tabs to delimit multiple domain names; commas are not valid delimiters.

- **Default IPv4 Gateway:** Use the corresponding field to specify the IPv4 address of the routing device where all packets are sent to destinations without an explicit route. The gateway is necessary when sending traffic to the Internet, to remotely managed devices, or for any other resource access. In a production environment, this value should not be "0.0.0.0" or empty.
- **Default IPv6 Gateway:** Use the corresponding field to specify the IPv6 address of the routing device where all packets are sent to destinations without an explicit route. The gateway is necessary when sending traffic to the Internet, to remotely managed devices, or for any other resource access. In a production environment, this value should not be empty.
- **DNS Servers:** Specify the name or IP address of one or more DNS servers (one per line to a maximum of three lines). The appliance only considers the first three entries due to restrictions on the underlying OS. For AWS and Azure deployments, the DNS servers of the hosting platform are displayed here, and cannot be changed.

**NOTE**

If you use a hostname for an NTP server, a DNS server is required here. If you remove all DNS servers, ensure that any configured NTP servers use IP addresses instead. See [Configure Date/Time Settings](#) for details.

- **MTU:** Enter a value, in bytes, for the maximum transmission unit (MTU) size, with a minimum value of 1000. The MTU value is updated instantly. You do **not** need to restart the network or reboot the appliance for the MTU value to take effect.

**NOTE**

Both the AWS and Azure platforms support updates to the MTU configuration. However, Microsoft states the preferred MTU is the default value of 1500. If the MTU is rejected by Azure network configuration, the MTU may reset to this default value.

- **IPv6 Enabled:** This option enables the IPv6 protocol in PAM. PAM can run on an IPv6 interface and can connect to target servers that are specified by IPv6 addresses for access or commercial management. Enabling or disabling this setting requires a reboot of your PAM device.
- **Network Interfaces:** This table defines network interfaces. The primary network interface is shown in the first row, named GB1. You use more network interfaces for specific features, such as [Additional Routes](#). To add another network interface, enter appropriate values in the **IPv4 Address**, **IPv6 Address**, **Netmask**, and **IPv6 CIDR** columns, in an available row, such as GB2. The following other columns are also present:
  - **Teaming:** Use this drop-down list to assign network interfaces to a Team. See [Network Teaming Interfaces](#) for more information.
  - **Speed:** Specifies the Ethernet capacity specification. Select **Auto** (negotiation), **1GB** (gigabit/sec), or **100** (100 megabit/sec). Default is Auto.
  - **Duplex:** Specifies the Ethernet transmission mode. Select **Auto** (negotiation), **Half** (half-duplex; alternating bidirectional), or **Full** (full-duplex; simultaneously bidirectional). Default is Auto.
  - **Enabled:** Specifies whether the interface is enabled.

**NOTE**

Licensing no longer includes the NIC to generate the hardware identification string. This change allows NICs to be added to running machines without breaking the licensing.

**Network Teaming Interfaces**

You can set up Network Teaming (also known as NIC teaming, bonding, or aggregation) to combine multiple network cards together for either enhanced performance or redundancy. A "bond" is set up among multiple network interfaces. This feature is available on the hardware appliance and VMware.

**NOTE**

NIC Teaming is available in VMware, configured in vSphere. Before you set up Network Teaming in Privileged Access Manager, ensure that no conflicts exist with the vSphere configuration.

**Modes**

Privileged Access Manager supports two Modes for Network Teaming:

- **Active Backup:** Use this mode for failover purposes. The first selected interface in the list (such as GB1) becomes the primary interface, and any others that are selected are "standby."
- **Adaptive Load Balancing:** Use this mode to increase throughput by sharing network traffic among several network interfaces.

## Configure Network Interface Bonds

Network interfaces are teamed together as a "bond." Privileged Access Manager supports up to four interfaces for teaming on a hardware appliance. On a VMware instance, you can use up to half of the existing teaming interfaces, or up to its maximum index. Assume that each VMware bond must have at least two interfaces. For example, if a VMware instance has seven network adapters, then the maximum allowed bond interfaces is three (BOND1, BOND2, and BOND3).

### Follow these steps:

1. Go to **Configuration, Network, Network Settings**.
2. Select a Network Teaming Interface bond, such as BOND1.
  - a. Enter an **IPv4** or **IPv6 Address** as a virtual network adapter for the bond.

#### NOTE

Each Bond should be configured to use a different subnet. Using the same subnet results in errors.

- b. For an IPv4 address, enter a **Netmask**, such as 255.255.255.0. For an IPv6 address, enter an **IPv6 CIDR** value.
  - c. Select a **Speed** from the drop-down list, or leave as "Auto."
  - d. Select a value for **Duplex** from the drop-down list, or leave as "Auto."
  - e. Select a **Mode** from the drop-down list, as described in [Modes](#).
3. In the list under Network Interfaces, select which interfaces should be teamed together with that bond.
  - a. For each interface, such as GB1 and GB2, select the bond from the **Teaming** drop-down list.
  - b. An Interface is automatically **Enabled** once it joins a team.
4. Select the **Update** button to save any changes. Select **Reset** to return the settings to their last saved state without saving. Select **Restart Networking** to start using the new settings immediately.

To see the status of a Network Team, select its row in the Network Teaming list, and select the **Status** button. The Network Team Status window opens. The following information appears:

- **Mode:** If mode is Active Backup, the Primary Interface (as opposed to the Backup interface) is listed. The Active Interface is the current active interface that sends and receives network traffic. If the Active Interface is not the same as Primary Interface, the Primary Interface is down and the failover has occurred.
- **Status:** A checkmark denoted that the team is operational.
- **Interfaces**
  - **Status:** A checkmark denoted that the interface is operational.
  - **Failure Count:** This number is a count of the failures of the member interface. This number is reset to zero when networking restarts or when the appliance reboots.

#### NOTE

- [Additional Routes](#)
- [Administrative Access Restriction](#)

## Restrict Administrative Access

By default, any user with administrator credentials can access the Configuration settings. To restrict access, explicitly specify which hosts have access by creating a white list.

### WARNING

When you add an IP address or CIDR block to the Access Restrictions settings, administrators on hosts that are not explicitly added are blocked from accessing the Configuration settings. For this reason, ensure that you add your own IP address.

You add an entry to the table, which functions as a whitelist.

**Follow these steps:**

1. Select **Configuration, Network, Access Restriction** to specify which networks or hosts can access the Configuration settings.
2. Select **Add**.  
The Add IP address / CIDR block window appears.
3. Enter an IP or CIDR block address to the text box. Examples: 192.168.1.1, 130.200.13.0/24
4. Select **OK**.  
The IP address or block of addresses is added to the list.  
Upon logging in again, only users having IP addresses included in the list can access the Configuration settings.

## Additional Routes

Select **Configuration, Network, Additional Routes** to configure routes to specific destinations. You can add routes for IPv4 and IPv6.

**Additional IPv4 Routes Tab**

- **Destination:** Specify the IP address or hostname for the destination of the route.
- **Netmask:** Enter a netmask, such as 255.255.255.0 . If **Netmask** is set to 255.255.255.255 , the target destination for the route is the network. Otherwise, the target destination for the route is host.
- **Gateway:** Specify the IP address of the routing device where all packets are sent to destinations without an explicit route.
- **Metric:** (optional) Lower values are preferred over higher
- **Device:** Assign an available Ethernet port, GB1 through GB3.

**Additional IPv6 Routes Tab**

- **Destination:** Specify the IP address or hostname for the destination of the route.
- **Gateway:** Specify the IP address of the routing device where all packets are sent to destinations without an explicit route.
- **Device:** Assign an available Ethernet port, GB1 through GB3.

## Configure Container Network Settings

**NOTE**

This topic was previously titled "Configure Docker Network Settings" because it described procedures that you performed on the **Docker Network Settings** panel. However, in this release (4.1.4) that screen has been renamed to **Container Network Settings** and this page has been renamed correspondingly.

Container technology allows applications and their dependencies to be packaged and run consistently across various computing environments. PAM uses this technology in the following components:

- PAM servers have an integrated *Local PAM Container* in which several PAM server components run.
- PAM SC Utility Appliances have an integrated *Utility Appliance Container* in which several Utility Appliance components run.

By default, all Local PAM Containers in the cluster use a virtual IPv4 network bridge to communicate with each other and their host PAM servers. By default, the IPv4 address range for the PAM server network bridge is 172.17.0.1/16 , so the container on each PAM server is assigned an IPv4 address in the 172.17.\*.\* range.

Alternatively, if you have configured a custom IPv6 subnet for Local PAM Containers, the default IPv6 CIDR value is f1b1:a:b:c::/64 .

Utility Appliance Containers use a separate IPv4 network bridge to communicate with each other and their host Utility Appliances. By default, the IPv4 address range for the Utility Appliance network bridge is `172.17.0.1/16`, so the container on each registered Utility Appliance is assigned an IPv4 address in the `172.17.*.*` range.

Use the following procedure to modify the default container bridge IP address ranges in case addressing conflicts occur. For example, using Classless Inter-Domain Routing (CIDR) for allocating IP addresses and routing in your environment can cause such conflicts.

**To modify the default container bridge IP ranges, follow these steps:**

1. Log into the PAM UI.
2. Navigate to **Configuration, Network, Container Network Settings**.
3. Update the value in the corresponding field:
  - **Local PAM Container IPv4 network bridge**: Enter an IPv4 address range. For example, `172.17.0.8/20`. The default value is `172.17.0.1/16`.
  - **Local PAM Container IPv6 Subnet CIDR**: Enter an IPv6 Subnet CIDR. For example, `f2b2:a:b:c::/64`. The default value is `f1b1:a:b:c::/64`.

#### NOTE

If you observe any issues with PAM or Utility Appliance operations after updating the Local PAM IPv6 Container CIDR, restart PAM networking. Specifically, restart PAM networking if any of the following conditions occur:

- Log forwarding to the splunk or syslog server is not functioning correctly.
- Target applications and accounts, especially the Active Directory SSH Key type are not functioning correctly
- An error appears while accessing the **Configuration, Utility, Status, Utility Group Status** page in the PAM UI.

**To restart PAM networking:** Navigate to **Configuration, Network, Network Settings** and select the **Restart Networking** button.

- **Utility Appliance Container IPv4 network bridge**: Enter an IPv4 address range. For example, `172.17.0.8/20`. The default value is `172.17.0.1/16`.
4. Select the **Update** button beside the value that you modified to apply the change.

The container configuration file is updated and the container daemon (`/etc/docker/daemon.json`) restarts.

#### NOTE

There may be temporary interruption in operation while the container daemon restarts. During this time, the **Update** button grays out. If you modified the Local PAM Container IPv4 or IPv6 values, the **local PAM container Daemon Status** informational field displays the condition of the Local PAM Container daemon.

## Custom Host File Entries

This feature enables users to update the PAM host file from the PAM user interface. In a clustered environment, host file entries are replicated across the cluster nodes and take 60 seconds at the most to replicate.

**Follow these steps:**

1. Select **Configuration, Network, Host File Entry**.
2. Select **Add**.  
The Add Host File Entry window appears.
3. Enter an IP address.

- IPv4 example: 10.11.12.13
  - IPv6 example: fd6d:8d64:af0c:1:0:242:22:233  
IPv6 addresses can be up to 40 characters.
4. Add one or more host names. Select the plus symbol to add additional hosts names. Select the x symbol to delete a host name.
  5. Add any optional comments about the host file entry.
  6. Select **OK**.  
A host file entry is added to the list.

## Authorize SNMP Polling

As a network administrator, you can authorize Simple Network Management Protocol (SNMP) polling of Privileged Access Manager.

### Follow these steps:

1. Go to **Configuration, SNMP, Poll Server**.
2. To respond only to SNMP version 3 requests, select the **SNMP V3 Only** checkbox.  
SNMP version 2c does not use encryption, and version 3 is required for **FIPS Mode**.
3. The **Read-Only Community** string is required only for SNMP version 2c, and is used for authentication.  
The current string is shown in this field, and you can edit it when the **SNMP V3 Only** checkbox is not selected.
4. Select **Start at Boot** to start a poll server when the appliance starts.
5. Select **Save** to save your settings.
6. Select **Start** to start the service immediately.  
The **Server Status** field reflects that it is running.  
You can select **Stop** to stop the service.

## Add SNMP V3 Users

As a network administrator, you can add polling user credentials to support SNMP v3 polling of Privileged Access Manager. To add an SNMP V3 user, follow these steps:

1. Go to **Configuration, SNMP, SNMP V3 Users**.
2. Select the **Add** button.  
The **Add SNMP User** window appears.
3. Enter the values for the user:
  - a. **Username** - Specify the user name to be authenticated with polling. Do not use the reserved user "xceedium".
  - b. **Authentication Passphrase** - Specify the public passphrase to be used with polling.
  - c. **Confirm Auth Passphrase** - Retype the public passphrase to confirm.
  - d. **Private Passphrase** - Specify the private passphrase to be used with polling.
  - e. **Confirm Private Passphrase** - Retype the private passphrase to confirm.
4. Select the **OK** button.

To edit an existing SNMP user, select the user from the list and select **Update**. To delete a user, select **Delete**.

## Enable SNMP Traps

As a network administrator, you can enable Simple Network Management Protocols (SNMP) traps on Privileged Access Manager. Configure access to an SNMP trap server using the Trap Server configuration page. Follow these steps:

1. Go to **Configuration, SNMP, Trap Server**.
2. Select the **Traps Enabled** checkbox.

3. Enter the **Trap Community** string that is used for authentication.

**NOTE**

The default **xcdgkpub** community retrieves the full MIB (Management Information Base). Starting with Privileged Access Manager 3.0, which is built on Debian 8, the "public" community retrieves only system information. In some earlier versions, the "public" community did retrieve the full MIB, but starting in Privileged Access Manager 3.0, use the **xcdgkpub** community to get the full MIB.

4. Specify the IP address or hostname of the **Traps Destination** server, also known as the Network Management Server.
5. Select **SNMP Version** 2c or 3.

**NOTE**

**FIPS Mode** does not support SNMP Version 2c. Use SNMP Version 3 with FIPS Mode.

6. For **SNMP V3**, enter these values:
  - a. **SNMPv3 Username**
  - b. **SNMPv3 Passphrase**
  - c. **SNMPv3 Private Passphrase**
7. Select the **Save Configuration** button.

### **Trap Server Internal Configuration**

**NOTE**

Privileged Access Manager uses SNMP **Inform**s rather than **Traps**.

- **Inform**s use acknowledgments for their notifications, whereas Traps do not.
- With **Inform**s in SNMPv3, the receiving application is authoritative, rather than the sending application (Privileged Access Manager).

When you configure an SNMPv3 Trap Server to receive traps from Privileged Access Manager, use the following values:

- authProtocol: SHA
- privProtocol: AES
- securityLevel: AuthPriv

## **Management Information Base (MIB) for SNMP Use**

A Management Information Base (MIB) describes the format of Simple Network Management Protocol (SNMP) messages for an organization. The attached MIB file contains the configuration for a network management program to receive Privileged Access Manager SNMP event notifications.

The following sections contain detailed lists of the Notifications, Object Types, MIB objects, and their Object Identifiers (OIDs). The final section describes some sample SNMP output.

The MIB text file contains most of this information. You can [view it](#) or you can [download it](#) by right-clicking and selecting the Save As option.

The Base OID for the Privileged Access Manager MIB is 1.3.6.1.4.1.10449.

### **Severity**

The `gkAlarmPerceivedSeverity` object (OID 406, as described in [Object Types](#)) in the SNMP notifications contains an integer denoting its severity:

Integer	Perceived Severity
0	indeterminate



1	critical
2	major
3	minor
4	warning
5	cleared

### Notification Types

The following table contains a list of notification types that are exposed as objects in the MIB. These objects are under `xceediumNotifications`.

Notification Type	Description	OID
<code>gkGenericNotification</code>	Generic type Xsuite Notification (unspecified)	100
<code>gkSysSMBServerStatus</code>	Remote Samba resource status	101
<code>gkSysNFSServerStatus</code>	Remote NFS resource status	102
<code>gkSysLDAPServerStatus</code>	LDAP server status	103
<code>gkSysSyslogServerStatus</code>	Remote syslog server status	104
<code>gkSysMailServerStatus</code>	Remote SMTP server (relay) status	105
<code>gkSysClusterStatus</code>	This notification is sent when the cluster status changes.	107
<code>gkSysDbBackupSMBServerStatus</code>	Remote Samba database backup resource status	108
<code>gkSysDbBackupNFSServerStatus</code>	Remote NFS database backup resource status	109
<code>gkSysDbBackupS3ServerStatus</code>	Remote S3 database backup resource status	110
<code>gkSysMultiSiteStatus</code>	Multisite cluster status changes	112
<code>gkSysS3ServerStatus</code>	Remote S3 resource status	113
<code>gkSessLoginFailed</code>	Login to Xsuite failed	200
<code>gkSessConnTerminated</code>	Xsuite connection session terminated	201
<code>gkSessLoginTerminated</code>	Xsuite Login session terminated	202
<code>gkSessConnExpired</code>	Xsuite connection session expired and is terminated	203
<code>gkSessLoginExpired</code>	Xsuite login session expired and is terminated	204
<code>gkSessSessRecAlert</code>	Xsuite session recording alert	205
<code>gkSessSessRecViolation</code>	Xsuite session recording violation	206
<code>gkSessSFAccDeactivated</code>	Account deactivated because of Xsuite socket filtering (leapfrog prevention) violation	207
<code>gkSessSFViolation</code>	Xsuite socket filtering (leapfrog prevention) violation	208



gkSessCFAlert	Xsuite command filtering alert	209
gkSessCFViolation	Xsuite command filtering violation	210
gkSessCFAccDeactivated	Account deactivated because of Xsuite command filtering violation	211
gkAppGKMonitorStatus	Xsuite monitor process started	300
gkAppLogwatchStatus	Logwatch process started	301
gkAppSNMPAgentStatus	Xsuite SNMP agent started	302
gkAppSNMPSubagentStatus	Status of the SNMP subagent, used to reply to polls of the Xceedium MIB OIDs	303
gkAppDBStatus	Xsuite database is up	304
gkAppFWDStatus	Xsuite secure forwarder started	305
gkAppSessManagerStatus	Xsuite session manager is started	306
gkAppAPWDStatus	Xsuite application watchdog daemon started	310
gkAppGKAuthDStatus	Xsuite application authentication daemon exception	311

### **Object Types**

The following table describes the properties that can be sent in the various notifications.

<b>Object Name</b>	<b>Syntax</b>	<b>Description</b>	<b>OID</b>
gkTrapUsername	DisplayString	Name of the user logged in at the time of the trap.	400
gkTrapDeviceIP	DisplayString	IP Address of the device on Xsuite where the trap occurred.	401
gkTrapDescription	DisplayString	Description of the trap.	402
gkAlarmEventTime	DateAndTime	This object represents the time of occurrence of the subject alarm. The time indication is in Xsuite local time.	403

gkAlarmId	Integer32	This object uniquely identifies an entry in the Alarm Table. It increases every time a new alarm occurs. Due to cleared alarms the index will not be contiguous. When the maximum is reached of Integer32 , the value of this object rolls over to 1. The actor must use 'alarmEventTime' to sort on chronological order. The gkAlarmId object is read-only even though it is used as index in the Alarm Table. The reason is that this facilitates a convenient way to extract the corresponding value from a notification where the object is included.	404
gkAlarmProbableCause	ProbableCause	This object represents the probable cause identification code (generic classification) for the subject alarm.	405
gkAlarmPerceivedSeverity	PerceivedSeverity	This object represents the perceived severity of the subject alarm.	406
gkAlarmName	DisplayString	The name of the event or alarm.	407
gkAlarmObject	DisplayString	The alarming object.	408
gkAlarmInformation	DisplayString	Additional information pin-pointing the problem.	409

## Status

The following table contains the subset of status properties that are exposed as objects in the MIB. These objects are under gkStatus for xceediumGateKeeper , and belong to the gkStatusGroup (group OID 4).

Object Identity	Syntax	Description	OID
gkSystemSerialNumber	DisplayString	Xsuite System Serial number, which is used to license the Xsuite and is tied to the security of the system	1
gkHardwareSerialNumber	DisplayString	Hardware Serial number of the Xsuite appliance, which is used to track the physical Xsuite hardware. The system Serial number may change in time, depending on the current circumstances, which in term will require a change in the license string.	2

gkVersion	DisplayString	Xsuite firmware version. This is the version number, which only shows which base firmware version is installed on the box. To determine what is the exact firmware configuration see the applied patches on the box.	3
gkAppliedPatches	DisplayString	All patches (hot-fixes, service packs or special patches) applied to the Xsuite appliance, showing as name with date and time	4
gkLicenseNodes	Integer32	Number of devices licensed for Access.	5
gkLicensesUtilized	Integer32	Number of Access licenses utilized out of the maximum issued.	6
gkTotalUsers	Integer32	Total number of users registered in the Xsuite database.	7
gkLoggedInUsers	Integer32	Displays the number of the currently logged in users	8
gkCurrentSessions	Integer32	Displays the number of the current sessions to remote hosts	9
gkTotalDBDiskUsage	Integer32	Disk space, occupied by the Xsuite database	10
gkLogDiskSize	Integer32	Current size of the logs on the disk	11
gkLogRecords	Integer32	Current number of the Xsuite log records	12
gkClusterStatus	DisplayString	Status of the GK if in cluster mode	13
gkMainframeStatus	DisplayString	Status of the Mainframe licensing.	15
gkAWSStatus	DisplayString	Status of the AWS licensing.	16
gkVMwareStatus	DisplayString	Status of the VMware licensing.	17
gkPassLicenseNodes	Integer32	Number of devices licensed for Password Authority.	18
gkPassLicensesUtilized	Integer32	Number of Password Authority licenses utilized out of the maximum issued.	19
gkA2ALicenseNodes	Integer32	Number of devices licensed for A2A.	20
gkA2ALicensesUtilized	Integer32	Number of A2A licenses utilized out of the maximum issued.	21
gkOffice365Status	DisplayString	Status of the Office365 licensing.	22

gkSafeNetHSMStatus	DisplayString	Status of the SafeNet HSM licensing.	23
gkThalesHSMStatus	DisplayString	Status of the Entrust HSM licensing.	24

## Alarms

The following table describes the basic alarm notifications that are sent by Privileged Access Manager.

Notification Type	Objects	Description	OID
gkAlarmStartup	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Xsuite is starting up.	500
gkAlarmShutdown	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Xsuite is shutting down.	501
gkAlarmReboot	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Xsuite is rebooting.	502
gkAlarmLinkUP	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Link on Xsuite has come up.	503
gkAlarmLinkDown	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Link on Xsuite has gone down.	504

## Hardware Monitoring

The following table describes notifications specific to the Privileged Access Manager hardware appliance. These objects are from `xcd_hwmon`.

Notification Type	Objects	Description	OID
<code>gkCpuTempFailure</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	The CPU temperature has gone above 135°F.	600
<code>gkCpuTempRecovery</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	The CPU temperature has returned to below 135°F.	601
<code>gkChassisFanFailure</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	One or more of the chassis fans have failed.	602
<code>gkChassisFanRecovery</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	All of the chassis fans have recovered from their failure states.	603
<code>gkPrimaryDriveFailure</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	The primary SSD has failed.	604
<code>gkPrimaryDriveRecovery</code>	<code>gkAlarmId,</code> <code>gkAlarmName,</code> <code>gkAlarmEventTime,</code> <code>gkAlarmPerceivedSeverity,</code> <code>gkAlarmObject,</code> <code>gkAlarmProbableCause,</code> <code>gkAlarmInformation</code>	The primary SSD has recovered from its failure.	605

gkSecondaryDriveFailure	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The secondary SSD has failed.	606
gkSecondaryDriveRecovery	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The secondary SSD has recovered from its failure.	607
gkPrimaryPsuFailure	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The primary (leftmost) PSU has been removed or failed.	608
gkPrimaryPsuRecovery	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The primary (leftmost) PSU has been re-inserted or recovered from its failure.	609
gkSecondaryPsuFailure	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The secondary (rightmost) PSU has been removed or failed.	610
gkSecondaryPsuRecovery	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	The secondary (rightmost) PSU has been re-inserted or recovered from its failure.	611
gkTotalDiskUsageStatus	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Total disk used status	700

gkTotalDBDiskUsageStatus	gkAlarmId, gkAlarmName, gkAlarmEventTime, gkAlarmPerceivedSeverity, gkAlarmObject, gkAlarmProbableCause, gkAlarmInformation	Total database disk used status	701
--------------------------	---	---------------------------------	-----

### Sample Notification

Line breaks have been added to this sample output. The service status section only appears when the service is started. The message body is divided into object-value pairs, such as OID 10449.0.403, `gkAlarmEventTime`, as described in the [Object Types](#) table. The date and time value is expressed as a hex string. The first two octets represent the year. In this case, `07E2` is 2018. The year is followed by month (`0C` is 12 for December), day, hour, minute, second, and deciseconds. The final OID, 10449.0.406, indicates the [Severity](#) as "critical."

```
[user@test01 snmp]# service snmptrapd status -l
```

```
Redirecting to /bin/systemctl status -l snmptrapd.service
```

- `snmptrapd.service` - Simple Network Management Protocol (SNMP) Trap Daemon.

```
Loaded: loaded (/usr/lib/systemd/system/snmptrapd.service; disabled; vendor preset: disabled)
```

```
Active: active (running) since Thu 2018-12-06 12:37:53 EST; 3h 25min ago
```

```
Main PID: 34413 (snmptrapd)
```

```
CGroup: /system.slice/snmptrapd.service
```

```
└─34413 /usr/sbin/snmptrapd -Lsd -f
```

```
Dec 06 14:01:36 test01 snmptrapd[34413]: 2018-12-06 14:01:36 capam32.test.com [UDP: [0.0.0.0]:50946->[0.0.0.0]:162]:
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2500) 0:00:25.00
```

```
SNMPv2-MIB::snmpTrapOID.0 = OID:
```

```
SNMPv2-SMI::enterprises.10449.0.504
```

```
SNMPv2-SMI::enterprises.10449.0.402 = STRING: "GB2 (eth1) has gone down"
```

```
SNMPv2-SMI::enterprises.10449.0.405 = STRING: "A network interface has gone down."
```

```
SNMPv2-SMI::enterprises.10449.0.407 = STRING: "gkAlarmLinkDown"
```

```

SNMPv2-SMI::enterprises.10449.0.408 = STRING: "Xsuite"

SNMPv2-SMI::enterprises.10449.0.409 = STRING: "A network interface has gone down."

SNMPv2-SMI::enterprises.10449.0.403 = Hex-STRING: 07 E2 0C 06 13 00 30 00

SNMPv2-SMI::enterprises.10449.0.404 = INTEGER: 71

SNMPv2-SMI::enterprises.10449.0.406 = INTEGER: 1

```

## NOTE

Download the MIB from [here](#).

## XCEEDIUM-MIB File

To obtain the PAM MIB file, copy the text in the following code box into a text editor and save it as XCEEDIUM-MIB.txt. For more information, see [Management Information Base \(MIB\) for SNMP Use](#).

```

XCEEDIUM-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-IDENTITY,
    OBJECT-TYPE
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC
    TEXTUAL-CONVENTION, DateAndTime
        FROM SNMPv2-TC
    ;

--=====
-- TEXTUAL CONVENTIONS
--=====

xceedium MODULE-IDENTITY
    LAST-UPDATED "201905100000Z" -- May 10, 2019
    ORGANIZATION
        "Xceedium, Inc."
    CONTACT-INFO
        "Postal: Xceedium, Inc.
        2214 Rock Hill Road, Suite 100
        Herndon, VA 20170
        Web site: http://www.xceedium.com/"
    DESCRIPTION
        "Xceedium generic MIB"
    REVISION
        "201905100000Z"
    DESCRIPTION

```



"MIB objects incorrectly labeled"

REVISION

"201904120000Z"

DESCRIPTION

"Removal of obsolete MIB alerts"

REVISION

"201609280344Z"

DESCRIPTION

"Initial"

::= { 1 3 6 1 4 1 10449 }

PerceivedSeverity ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Perceived severity as specified in ITU  
recommendation X.733. The value indeterminate(0)  
is not recommended to be used."

SYNTAX INTEGER {

indeterminate(0),  
critical(1),  
major(2),  
minor(3),  
warning(4),  
cleared(5)

}

ProbableCause ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Probable cause of the alarm."

SYNTAX OCTET STRING (SIZE (0..200))

ProductID ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"This is the identification of the product"

SYNTAX OBJECT IDENTIFIER

xceediumCompliance MODULE-COMPLIANCE

STATUS current

DESCRIPTION

"This is the Xceedium module compliance."

MODULE XCEEDIUM-MIB

MANDATORY-GROUPS

{ gkAccessNotifGroup, gkAppNotifGroup, gkStatusGroup,  
gkSystemNotifGroup }

::= { 1 0 }

xceediumNotifications OBJECT-IDENTITY

STATUS current

DESCRIPTION

"Xsuite traps and notification"

```
::= { xceedium 0 }

gkGenericNotification NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Generic type Xsuite Notification (unspecified)"
    ::= { xceediumNotifications 100 }

gkSysSMBServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Remote Samba resource status"
    ::= { xceediumNotifications 101 }

gkSysNFSServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Remote NFS resource status"
    ::= { xceediumNotifications 102 }

gkSysLDAPServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "LDAP server status"
    ::= { xceediumNotifications 103 }

gkSysSyslogServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Remote syslog server status"
    ::= { xceediumNotifications 104 }

gkSysMailServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Remote SMTP server (relay) status"
    ::= { xceediumNotifications 105 }

gkSysClusterStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "This notification is sent when the cluster status changes."
    ::= { xceediumNotifications 107 }

gkSysDbBackupSMBServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Remote Samba database backup resource status"
    ::= { xceediumNotifications 108 }

gkSysDbBackupNFSServerStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
```

```
"Remote NFS database backup resource status"
::= { xceediumNotifications 109 }

gkSysDbBackupS3ServerStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Remote S3 database backup resource status"
::= { xceediumNotifications 110 }

gkSysMultiSiteStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Multisite cluster status changes"
::= { xceediumNotifications 112 }

gkSysS3ServerStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Remote S3 resource status"
::= { xceediumNotifications 113 }

gkSessLoginFailed NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Login to Xsuite failed"
::= { xceediumNotifications 200 }

gkSessConnTerminated NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite connection session terminated"
::= { xceediumNotifications 201 }

gkSessLoginTerminated NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite Login session terminated"
::= { xceediumNotifications 202 }

gkSessConnExpired NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite connection session expired and is terminated"
::= { xceediumNotifications 203 }

gkSessLoginExpired NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite login session expired and is terminated"
::= { xceediumNotifications 204 }

gkSessSessRecAlert NOTIFICATION-TYPE
STATUS          current
```

```
DESCRIPTION
    "Xsuite session recording alert"
::= { xceediumNotifications 205 }

gkSessSessRecViolation NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Xsuite session recording violation"
    ::= { xceediumNotifications 206 }

gkSessSFAccDeactivated NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Account deactivated because of Xsuite socket filtering (leapfrog prevention) violation"
    ::= { xceediumNotifications 207 }

gkSessSFViolation NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Xsuite socket filtering (leapfrog prevention) violation"
    ::= { xceediumNotifications 208 }

gkSessCFAlert NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Xsuite command filtering alert"
    ::= { xceediumNotifications 209 }

gkSessCFViolation NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Xsuite command filtering violation"
    ::= { xceediumNotifications 210 }

gkSessCFAccDeactivated NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Account deactivated because of Xsuite command filtering violation"
    ::= { xceediumNotifications 211 }

gkAppGKMonitorStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Xsuite monitor process started"
    ::= { xceediumNotifications 300 }

gkAppLogwatchStatus NOTIFICATION-TYPE
    STATUS          current
    DESCRIPTION
        "Logwatch process started"
    ::= { xceediumNotifications 301 }

gkAppSNMPAgentStatus NOTIFICATION-TYPE
```

```

STATUS          current
DESCRIPTION
    "Xsuite SNMP agent started"
::= { xceediumNotifications 302 }

gkAppSNMPSubagentStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Status of the SNMP subagent, used to reply to polls of the
    Xceedium MIB OIDs"
::= { xceediumNotifications 303 }

gkAppDBStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite database is up"
::= { xceediumNotifications 304 }

gkAppFWDStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite secure forwarder started"
::= { xceediumNotifications 305 }

gkAppSessManagerStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite session manager is started"
::= { xceediumNotifications 306 }

gkAppAPWDStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite application watchdog daemon started"
::= { xceediumNotifications 310 }

gkAppGKAuthDStatus NOTIFICATION-TYPE
STATUS          current
DESCRIPTION
    "Xsuite application authentication daemon exception"
::= { xceediumNotifications 311 }

gkTrapUsername OBJECT-TYPE
SYNTAX          DisplayString
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Name of the user logged in at the time of the trap."
::= { xceediumNotifications 400 }

gkTrapDeviceIP OBJECT-TYPE
SYNTAX          DisplayString
MAX-ACCESS      read-only

```

```

STATUS      current
DESCRIPTION
    "IP Address of the device on Xsuite where the trap occurred."
::= { xceediumNotifications 401 }

gkTrapDescription OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Description of the trap."
    ::= { xceediumNotifications 402 }

gkAlarmEventTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "This object represents the time of occurrence of the
        subject alarm. The time indication is in Xsuite local time."
    ::= { xceediumNotifications 403 }

gkAlarmId OBJECT-TYPE
    SYNTAX      Integer32 (0..2147483647)
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "This object uniquely identifies an entry in the
        Alarm Table. It increases every time a new alarm
        occurs. Due to cleared alarms the index will not be
        contiguous. When the maximum is reached of
        Integer32, the value of this object rolls over to 1.
        The actor must use 'alarmEventTime' to sort on
        chronological order.
        The gkAlarmId object is read-only even though it
        is used as index in the Alarm Table. The reason is
        that this facilitates a convenient way to extract
        the corresponding value from a notification where
        the object is included."
    ::= { xceediumNotifications 404 }

gkAlarmProbableCause OBJECT-TYPE
    SYNTAX      ProbableCause
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "This object represents the probable cause
        identification code (generic classification) for the
        subject alarm."
    ::= { xceediumNotifications 405 }

gkAlarmPerceivedSeverity OBJECT-TYPE
    SYNTAX      PerceivedSeverity

```

```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "This object represents the perceived severity of
    the subject alarm."
::= { xceediumNotifications 406 }

```

```

gkAlarmName OBJECT-TYPE
SYNTAX        DisplayString
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "The name of the event or alarm."
::= { xceediumNotifications 407 }

```

```

gkAlarmObject OBJECT-TYPE
SYNTAX        DisplayString
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "The alarming object."
::= { xceediumNotifications 408 }

```

```

gkAlarmInformation OBJECT-TYPE
SYNTAX        DisplayString
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "Additional information pin-pointing the problem."
::= { xceediumNotifications 409 }

```

```

gkAlarmStartup NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,
               gkAlarmInformation }
STATUS        current
DESCRIPTION
    "Xsuite is starting up."
::= { xceediumNotifications 500 }

```

```

gkAlarmShutdown NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,
               gkAlarmInformation }
STATUS        current

```

```

DESCRIPTION
    "Xsuite is shutting down."
::= { xceediumNotifications 501 }

gkAlarmReboot NOTIFICATION-TYPE
OBJECTS {
    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS      current
DESCRIPTION
    "Xsuite is rebooting."
::= { xceediumNotifications 502 }

gkAlarmLinkUP NOTIFICATION-TYPE
OBJECTS {
    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS      current
DESCRIPTION
    "Link on Xsuite has came up."
::= { xceediumNotifications 503 }

gkAlarmLinkDown NOTIFICATION-TYPE
OBJECTS {
    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS      current
DESCRIPTION
    "Link on Xsuite has gone down."
::= { xceediumNotifications 504 }

-- -----
-- Hardware Monitoring (xcd_hwmon) Traps
-- -----

gkCpuTempFailure NOTIFICATION-TYPE
OBJECTS {
    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,

```



```
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"The CPU temperature has gone above 135°F."
::= { xceediumNotifications 600 }

gkCpuTempRecovery NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"The CPU temperature has returned to below 135°F."
::= { xceediumNotifications 601 }

gkChassisFanFailure NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"One or more of the chassis fans have failed."
::= { xceediumNotifications 602 }

gkChassisFanRecovery NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"All of the chassis fans have recovered from their failure states."
::= { xceediumNotifications 603 }

gkPrimaryDriveFailure NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
```

```
STATUS    current
DESCRIPTION
"The primary SSD has failed."
::= { xceediumNotifications 604 }

gkPrimaryDriveRecovery NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"The primary SSD has recovered from its failure."
::= { xceediumNotifications 605 }

gkSecondaryDriveFailure NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"The secondary SSD has failed."
::= { xceediumNotifications 606 }

gkSecondaryDriveRecovery NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
DESCRIPTION
"The secondary SSD has recovered from its failure."
::= { xceediumNotifications 607 }

gkPrimaryPsuFailure NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS    current
```

```

DESCRIPTION
"The primary (leftmost) PSU has been removed or failed."
::= { xceediumNotifications 608 }

gkPrimaryPsuRecovery NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,
               gkAlarmInformation }
STATUS      current
DESCRIPTION
"The primary (leftmost) PSU has been re-inserted or recovered from its failure."
::= { xceediumNotifications 609 }

gkSecondaryPsuFailure NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,
               gkAlarmInformation }
STATUS      current
DESCRIPTION
"The secondary (rightmost) PSU has been removed or failed."
::= { xceediumNotifications 610 }

gkSecondaryPsuRecovery NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,
               gkAlarmInformation }
STATUS      current
DESCRIPTION
"The secondary (rightmost) PSU has been re-inserted or recovered from its failure."
::= { xceediumNotifications 611 }

-- -----
-- Disk Status Traps --
-- -----

gkTotalDiskUsageStatus NOTIFICATION-TYPE
OBJECTS {      gkAlarmId,
               gkAlarmName,
               gkAlarmEventTime,
               gkAlarmPerceivedSeverity,
               gkAlarmObject,
               gkAlarmProbableCause,

```

```

    gkAlarmInformation }
STATUS      current
DESCRIPTION
    "Total disk used status"
::= { xceediumNotifications 700 }
gkTotalDBDiskUsageStatus NOTIFICATION-TYPE
OBJECTS {    gkAlarmId,
    gkAlarmName,
    gkAlarmEventTime,
    gkAlarmPerceivedSeverity,
    gkAlarmObject,
    gkAlarmProbableCause,
    gkAlarmInformation }
STATUS      current
DESCRIPTION
    "Total database disk used status"
::= { xceediumNotifications 701 }

```

```

-----

xceediumObjects OBJECT IDENTIFIER ::= { xceedium 1 }

xceediumStats OBJECT IDENTIFIER ::= { xceediumObjects 1 }

xceediumConfig OBJECT IDENTIFIER ::= { xceediumObjects 2 }

xceediumGateKeeper OBJECT IDENTIFIER ::= { xceediumObjects 3 }

gkStatus OBJECT-IDENTITY
STATUS      current
DESCRIPTION
    "These values show the current status of the Xsuite."
::= { xceediumGateKeeper 1 }

gkSystemSerialNumber OBJECT-TYPE
SYNTAX      DisplayString
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Xsuite System Serial number, which is used to license the
    Xsuite and is tied to the security of the system"
::= { gkStatus 1 }

```

```

gkHardwareSerialNumber OBJECT-TYPE
SYNTAX      DisplayString
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Hardware Serial number of the Xsuite appliance, which is used to
    track the physical Xsuite hardware. The system Serial
    number may change in time, depending on the current
    circumstances, which in term will require a change in the
    license string."

```

```

::= { gkStatus 2 }

gkVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Xsuite firmware version

        This is the version number, which only shows which base firmware
        version is installed on the box. To determine what is the exact
        firmware configuration see the applied patches on the box."
    ::= { gkStatus 3 }

gkAppliedPatches OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "All patches (hot-fixes, service packs or special patches)
        applied to the Xsuite appliance, showing as name with date and time"
    ::= { gkStatus 4 }

gkLicenseNodes OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Number of devices licensed for Access."
    ::= { gkStatus 5 }

gkLicensesUtilized OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Number of Access licenses utilized out of the maximum issued."
    ::= { gkStatus 6 }

gkTotalUsers OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Total number of users registered in the Xsuite database."
    ::= { gkStatus 7 }

gkLoggedInUsers OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Displays the number of the currently logged in users"

```

```
 ::= { gkStatus 8 }

gkCurrentSessions OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Displays the number of the current sessions to remote hosts"
    ::= { gkStatus 9 }

gkTotalDBDiskUsage OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Disk space, occupied by the Xsuite database"
    ::= { gkStatus 10 }

gkLogDiskSize OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current size of the logs on the disk"
    ::= { gkStatus 11 }

gkLogRecords OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current number of the Xsuite log records"
    ::= { gkStatus 12 }

gkClusterStatus OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Status of the GK if in cluster mode"
    ::= { gkStatus 13 }

gkMainframeStatus OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Status of the Mainframe licensing."
    ::= { gkStatus 15 }

gkAWSStatus OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
```

```
STATUS          current
DESCRIPTION
    "Status of the AWS licensing."
::= { gkStatus 16 }

gkVMwareStatus OBJECT-TYPE
SYNTAX          DisplayString
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Status of the VMware licensing."
::= { gkStatus 17 }

gkPassLicenseNodes OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Number of devices licensed for Password Authority."
::= { gkStatus 18 }

gkPassLicensesUtilized OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Number of Password Authority licenses utilized out of the maximum issued."
::= { gkStatus 19 }

gkA2ALicenseNodes OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Number of devices licensed for A2A."
::= { gkStatus 20 }

gkA2ALicensesUtilized OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Number of A2A licenses utilized out of the maximum issued."
::= { gkStatus 21 }

gkOffice365Status OBJECT-TYPE
SYNTAX          DisplayString
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Status of the Office365 licensing."
::= { gkStatus 22 }
```

```

gkSafeNetHSMStatus OBJECT-TYPE
    SYNTAX          DisplayString
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Status of the SafeNet HSM licensing."
    ::= { gkStatus 23 }

gkThalesHSMStatus OBJECT-TYPE
    SYNTAX          DisplayString
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Status of the Thales HSM licensing."
    ::= { gkStatus 24 }

xceediumConformance OBJECT IDENTIFIER ::= { xceedium 2 }

xceediumCompliances OBJECT IDENTIFIER ::= { xceediumConformance 1 }

xceediumCapabilities OBJECT IDENTIFIER ::= { xceediumConformance 2 }

xceediumGroups OBJECT IDENTIFIER ::= { xceediumConformance 3 }

gkSystemNotifGroup NOTIFICATION-GROUP
    NOTIFICATIONS
        { gkGenericNotification, gkSysClusterStatus,
          gkSysLDAPServerStatus, gkSysS3ServerStatus,
          gkSysMailServerStatus, gkSysNFSServerStatus,
          gkSysSMBServerStatus, gkSysSyslogServerStatus,
          gkSysDbBackupNFSServerStatus, gkSysDbBackupSMBServerStatus,
          gkSysDbBackupS3ServerStatus }
    STATUS          current
    DESCRIPTION
        "System notification trap group"
    ::= { xceediumGroups 1 }

gkAccessNotifGroup NOTIFICATION-GROUP
    NOTIFICATIONS
        { gkSessCFAlert, gkSessCFViolation, gkSessConnExpired,
          gkSessConnTerminated, gkSessLoginExpired, gkSessLoginFailed,
          gkSessLoginTerminated, gkSessSessRecAlert,
          gkSessSessRecViolation, gkSessSFViolation }
    STATUS          current
    DESCRIPTION
        "Xsuite connection notification group"
    ::= { xceediumGroups 2 }

gkAppNotifGroup NOTIFICATION-GROUP
    NOTIFICATIONS
        { gkAppAPWDStatus, gkAppDBStatus, gkAppFWDStatus,
          gkAppGKAuthDStatus, gkAppGKMonitorStatus, gkAppLogwatchStatus,
          gkAppSessManagerStatus, gkAppSNMPAgentStatus, gkAppSNMPSubagentStatus }

```



```

STATUS          current
DESCRIPTION
    "Xsuite application notification group"
::= { xceediumGroups 3 }

gkStatusGroup OBJECT-GROUP
OBJECTS
    { gkAppliedPatches, gkClusterStatus,
      gkCurrentSessions, gkHardwareSerialNumber,
      gkLicenseNodes, gkLicensesUtilized, gkLogDiskSize,
      gkLoggedInUsers, gkLogRecords, gkSystemSerialNumber,
      gkTotalDBDiskUsage, gkTotalUsers, gkVersion }
STATUS          current
DESCRIPTION
    "This group contains the Xsuite status objects"
::= { xceediumGroups 4 }

END

```

## Configure Web Proxy Definitions

This content introduces web proxies and describes how to configure *web proxy definitions* to represent physical (or virtual) web proxies in your network. Use web proxy definitions when configuring [services to access web portals](#) if the network firewall would block a direct connection to the portal.

### NOTE

Web proxies are also referred to as web proxy servers and proxy servers.

### About Web Proxies

*Web proxies* act as an intermediary between devices inside your firewall and websites outside the firewall. A Network Administrator can configure one or more web proxies to allow controlled access to external websites that would otherwise be blocked by the firewall according to network security policy.

Web proxies can also be configured to provide the following security and performance benefits:

- Anonymize internal IP addresses to improve security.
- Caching content to improve data transfer speeds and reduce bandwidth usage.
- Filter content to prevent users from downloading content.

There are two methods to define web proxies in your environment:

- **Manual Configuration:** In a small environment, manually define proxy servers (by IP address and port).
- **Automatic Configuration:** In a large enterprise environment in which multiple web proxies are specified in a Proxy Auto-Configuraton (PAC) file, specify the URL of the PAC file.

### Configure a Web Proxy Definition

Use the following procedure to configure a web proxy definition to represent physical (or virtual) web proxies in your network.

#### Follow these steps:

1. Select **Configuration, Network, Web Proxies**.
2. Select the **Add** button.

3. Configure the following properties of the web proxy definition in the **Add Web Proxy** dialog that opens:
  - **Name:** A unique name for the web proxy definition.
  - **Description:** Optionally, a description of the web proxy definition.
  - **Proxy Type:** Specify the method to use to configure a proxy or multiple proxies, if they are defined in a PAC file. Select one of the following options:
    - **Use Manual Configuration:** Use this option to configure a single web proxy manually by specifying its host name or IP address and port in the **Address** and **Port** fields that appear.
    - **Use Automatic Configuration:** Use this option to configure multiple web proxies defined in a Proxy Auto-Configurator (PAC) file by specifying its URL in the **PAC URL** field. For example, `http://proxy1.company.com/proxy.pac`.
4. Select the **OK** button to save the web proxy definition.

**NOTE**

Specify a web proxy definition when configuring a service to access a web portal if the network firewall would otherwise block a direct connection to that portal. For more information, see [Configure a Service to Access a Web Portal](#).

## Configure Security Settings

This section describes how to configure security-related settings for your PAM environment, primarily using options under **Configuration**, **Security** in the PAM UI.

Use the table of contents to access the topics in this section.

### Server Access Options Configuration

As an administrator you specify the methods to use to access the server. You use the controls on **Configuration**, **Security**, **Access** to configure the server access methods.

#### Specify Access Options

Use the following controls on the **Access** tab to specify which methods to use to access the server.

**External REST API:** The External API provides programmatic control over most access functions. These functions include managing users, devices, and policies. This option also enables the API Doc interface. For more information, see [External API](#).

**Credential Management CLI:** The Credential Manager CLI provides administrative access to its password management functions. Management functions include adding, modifying, and deleting target and request data. The CLI also provides access to a limited set of maintenance operations. The Remote CLI is supported on UNIX, Linux, and Windows platforms. For more information, see [Use the Credential Manager CLI](#).

**VMware Console:** Access to the VMware console is enabled by default, and can be useful for emergency troubleshooting.

**Config User:** The product comes with a built-in Config user account, which you can disable. If you change the name of this account, you can still disable it.

**X-Forwarded-Host Check:** You can configure the appliance to deny any X-Forwarded-Host values that are not specified in a whitelist. Denying X-Forward host values protects against invalid host headers. To learn more about this option, see [Host Header Attack Mitigation](#).

**NOTE**

If your server is behind a proxy, load balancer, or router, verify that the device prevents against IP spoofing of the X-Forwarded-For HTTP header.

**Command String:** In addition to `sudo` and `pbrun` commands, you can enable command strings for Transparent Login to a managed device. Command strings are disabled by default as a security precaution. For more information, see [Device Setup, Transparent Login](#).

**TLS v1.0/1.1 Connection Allowed:** By default, the TLS 1.0, 1.1, and 1.2 communication protocols are enabled. To enhance security for inbound communication to PAM, such traffic from browsers, A2A clients, and the LDAP Browser, disable the **TLS v1.0/1.1 Connection Allowed** option. There may be existing connections using the TLS 1.0 or 1.1 protocol. Before you disable this setting, terminate any open connections TLS 1.0 or 1.1 connections by rebooting the appliance.

When FIPS mode is enabled, TLS 1.0 and TLS 1.1 protocols are automatically disabled. TLS 1.0 and TLS 1.1 are not permitted in FIPS mode.

#### NOTE

Applications running in the Java 6 runtime environment are limited to the TLS 1.0 protocol, such as version 2.8 A2A clients and Windows proxy agents. Update these components before disabling the **TLS v1.0/1.1 Communication Allowed** option. If your target server security upgrades allow only use of TLS 1.2 protocol, disable this setting.

**Concurrent Remote Connections:** By default, the appliance allows concurrent connections by the same user from different IP addresses. Your deployment might require concurrence. For example, a Citrix XenApp environment might have several jump boxes and a load balancer. An end user might run several sessions simultaneously, and the user sessions originate at different jump boxes.

To allow concurrent connections to a server, keep the default, **Enabled** for this option. To prevent concurrent connections to a server, set this option to **Disabled**.

#### IMPORTANT

In a clustered environment, setting **Concurrent Remote Connections** to **Disabled** does not prevent a user from having connections to other servers in the cluster. For example, if you have a cluster of five PAM servers, a user can have a single connection to all five of these servers, but cannot have multiple connections to any one of them.

### Specify PKI/Smart Card Options

To configure access options for smart card users, use the following controls on the **PKI/Smart Card Options** tab. For detailed configuration information, see [PKI Smart Card Authentication](#).

**PKI/Smart Card User Login:** With this option selected, the browser prompts for a client-side certificate upon locating the URL of the configured appliance.

**No Login Page without PKI/Smart Card:** When the Enabled checkbox is selected and a smart card is not present, users cannot to log in to the appliance. If the Disabled box is checked, users have the option of authenticating with Username and Password or other configured authentication methods. If users cannot authenticate with a smart card, the configuration page is always available with a known Username and Password.

**Policy Identifier:** Enter the PKI Policy Identifier here.

**Enable PKI/Smart Card Option on the Login Page:** If you use PKI smart cards to log in to PAM, this button adds a **PKI/Smart Card** option to the home page Authentication Type drop-down list.

## Secure Connections Using SSL Certificates

PAM uses TLS connections over HTTPS to secure communication between PAM servers and user sessions. You therefore require SSL certificates to enable these secure connections in your environment.

For a small test environment, you can create and use a self-signed SSL certificate.

For production environments including clusters, you require an SSL certificate from an in-house or third-party *Certificate Authority (CA)*.

You perform all certificate-related operations from the PAM UI **Configuration, Security, Certificates** page.

**See the following topics for detailed procedures for obtaining, applying, and managing SSL certificates:**

- [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#)
- [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#)
- [Obtain and Apply SSL Certificates for a Production Cluster](#)
- [Extract Required Certificates and CRLs from a Single SSL Certificate](#)
- [Certificate Revocation Update Options](#)
- [Sign Java Applets](#)
- [Delete a Certificate, CA Bundle, or CRL](#)

## Create a Self-Signed SSL Certificate for Use in a Testing Environment

As an administrator, you can create a self-signed SSL certificate, which is recommended as the minimal requirement to prevent security risk. This option is available at no cost, and useful for testing environments.

### NOTE

To obtain and install an SSL certificate for a single-server production environment, see [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#).

To obtain and install an SSL certificate for a clustered production environment, see [Obtain and Apply SSL Certificates for a Production Cluster](#).

For production environments, [Secure Connections Using SSL Certificates](#). Generating a Certificate Signing Request (CSR) requires more steps and might involve a cost. A CSR is ordinarily used when organization policy requires it. To generate a CSR and certificates for a cluster, see [Obtain and Apply SSL Certificates for a Production Cluster](#).

### Video Overview

This short video provides an overview of the procedure to create a self-signed certificate.

### Create the Self-Signed Certificate

Use this procedure to create a self-signed certificate.

#### **Follow these steps:**

1. in the PAM UI, navigate to **Configuration, Security, Certificates** page.  
Stay on the **Create** tab which opens by default.
2. Select the **Self-Signed Certificate** option for **Type**.
3. Enter information in the following fields. Only the fields with a red asterisk are required. Do not use special characters.

- **Key Size:** We recommend 2048 bits. 4096 bits is more secure, but it slows down TLS handshakes and increases processor load during handshakes.
- **Common Name:** Enter the FQDN or IP address of Privileged Access Manager for the certificate request, such as `capam.ca.com` or `10.144.39.187`. This field maps to the CN field of the X.509 certificate.
- **Country:** Enter the two-letter country code, such as US, FR, or JP. This field maps to C value of the X.509 certificate.
- **State:** Enter the optional State or Province, such as Illinois, or Quebec. This field maps to ST value of the X.509 certificate.
- **City:** Enter the optional locality or city designation, such as Paris or Islandia. This field maps to L value of the X.509 certificate.
- **Organization:** Enter the organization, typically a company, for the certificate, such as "Acme Technologies." This field maps to O value of the X.509 certificate.
- **Org. Unit:** Set the optional organizational unit name, typically a subdivision, or location of the Organization, such as "Security BU". This field maps to the OU value/Organizational Unit designation of the X.509 certificate.
- **Days:** Set the validity time-period. The current appliance date becomes the "Not Valid Before" date for the certificate. The "Days" field is then used to determine the "Not Valid After" date.
- **Use Common Name for SAN:** Because some browsers require a value in the **Alternative Subject Names** field, the Common Name is repeated there by default. To add more names in that field, clear this checkbox. The Common Name should still be repeated in the **Alternative Subject Names** field.
- **Alternative Subject Names:** Some browsers require a value in this field. If no value is specified, the Common Name is repeated here. If more than one address is used to access the appliance, list FQDN and IP address aliases to the Common Name, one per line. This list must include the Common Name. Do not add a newline (line feed) after the last entry. Refer to the X.509 Subject Alternative Name.

**NOTE**

**For clusters (in internal test environments only):** Add the FQDN and IP address for the VIP and every member of the cluster. Any hostname or short VIP name that is used to access the cluster should also be added.

- **Filename:** Create a name for the certificate.

**TIP**

Include the creation or expiration date in the filename. For example, name it `capam_exp2019-07-19`.

4. Select **Create**.  
A confirmation message appears at the top of the page.
5. Do the following steps to stage the certificate for use:
  - a. On the **Set** tab, select the filename of the certificate that you created previously. The `.crt` extension is added to your filename.
  - b. Select **Verify** to confirm that this certificate is acceptable by Privileged Access Manager.
  - c. Select **Accept** to switch to the new certificate.
  - d. Reboot the appliance for the new certificate to take effect.
  - e. Install the certificate as a trusted root certificate in a browser.
  - f. When the **Security Alert** pop-up window appears, select **View Certificate**.
  - g. When the **Certificate** pop-up window appears, select **Install Certificate**.

**NOTE**

PAM Agents version 3.4 and later support connecting to a PAM server with an unexpired, untrusted certificate. If an older version of the PAM Agent cannot connect to the server to download the updates, replace that agent with a newer version.

- h. Select the **Yes** button.

**NOTE**

**For related information, see the following topics:**

- [Secure Connections Using SSL Certificates](#)
- [Extract Required Certificates and CRLs from a Single SSL Certificate](#)
- [Certificate Revocation Update Options](#)
- [Sign Java Applets](#)
- [Delete a Certificate, CA Bundle, or CRL](#)

## Obtain and Apply SSL Certificates for a Single-Server Production Environment

This content describes how to obtain and apply SSL certificates from an in-house or third-party CA for a single-server production environment.

### NOTE

To obtain and install SSL certificates for a cluster, see [Obtain and Apply SSL Certificates for a Production Cluster](#).

To create and install a self-signed SSL certificate for a small development environment, see [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#).

### Video Overview

The following video provides a brief overview of this procedure.

Do the following procedures in order to obtain a certificate from a Certificate Authority (CA) and apply it your PAM server:

### Request a Certificate from a Certificate Authority

To create a Certificate Signing Request (CSR) request for one appliance, follow these steps:

1. On the Create tab of the **Certificates** page, select the **CSR** option for **Type**. Enter information for the following fields. Do not use special characters.
  - **Key Size:** We recommend 2048 bits. 4096 bits is more secure, but it slows down TLS handshakes and increases processor load during handshakes.
  - **Common Name:** Enter the FQDN or IP address of Privileged Access Manager for the certificate request, such as `pam.ca.com`, `10.144.39.187` (IPv4), or `fd6d:8d64:af0c:1:0:242:22:233` (IPv6). This field maps to the CN field of the X.509 certificate.
    - **For Clusters:** Enter the FQDN of the cluster Virtual IP address.
  - **Country:** Enter the two-letter country code, such as US, FR, or JP. This field maps to C value of the X.509 certificate.
  - **State:** Enter the optional State or Province, such as Illinois, or Quebec. This field maps to ST value of the X.509 certificate.
  - **City:** Enter the optional locality or city designation, such as Paris or Islandia. This field maps to L value of the X.509 certificate.
  - **Organization:** Enter the organization, typically a company, for the certificate, such as "Acme Technologies." This field maps to O value of the X.509 certificate.
  - **Org. Unit:** Enter the optional organizational unit name, typically a subdivision, or location of the Organization, such as "Security BU". This field maps to the OU value/Organizational Unit designation of the X.509 certificate.
  - **Days:** Days are used only for self-signed certificates.
  - **Use Common Name for SAN:** Because some browsers require a value in the **Alternative Subject Names** field, the Common Name is repeated there by default. To add more names in that field, clear this checkbox. The Common Name should still be repeated in the **Alternative Subject Names** field.
  - **Alternative Subject Names:** Some browsers require a value in this field. If no value is specified, the Common Name is repeated here. If more than one address is used to access the appliance, list FQDN and IP address aliases to the Common Name, one per line. This list must include the Common Name. Do not add a newline (line feed) after the last entry. Refer to the X.509 Subject Alternative Name.

- **For Clusters:** Enter the FQDN and IP address for the VIP and every member of the cluster. Any hostname or short VIP name that is used to access the cluster should also be added.
- **Filename:** Create a name for the certificate. This file name is also the name of the private key that is generated. The name must exactly match the name of the certificate when uploaded.

#### TIP

Include the creation or expiration date in the filename. For example, name it `capam_exp2019-07-19`.

2. Select **Create**.
3. On the **Download** tab, select the **Filename** of the CSR you created, which has a PEM (Privacy Enhanced Mail) extension.
4. Select **Download**.  
Submit the downloaded PEM file to request a certificate from your CA. Users do not have to install root certificates because the third party validates the site.
5. For clusters, remain on the **Download** tab to download the private key:
  - a. On the **Download** tab, select the Private Key from the **Filename** drop-down list. It is under the **Private Keys** heading, with the same name as the CSR, but a KEY extension.
  - b. Enter a **Password** and **Confirm Password** for encrypting the private key. Record this password to use later when uploading certificates to cluster members.
  - c. Select **Download**. Save the **Private Key** to add it later to the received Certificate for the other cluster members.
6. Obtain a new certificate using the downloaded CSR. Follow the instructions from your Certificate Authority to receive a certificate.

#### IMPORTANT

If the Certificate Authority provides all the required certificates and certificate revocation information in a single certificate file, follow the procedure that is described in [Extract Required Certificates and CRLs from a Single SSL Certificate](#) to extract them.

### Upload the Third-Party Certificates and CRLs

Once you have the certificates and CRLs for their chain of trust, you upload them into the PAM server. You must upload them in the right order to avoid errors:

1. Root certificate (as CA Bundle)
2. Intermediate CRL
3. Intermediate certificate
4. Device CRL
5. Device certificate

#### **Upload the Root Certificate**

1. Go to the **Configuration, Security, Certificates** page. Select the **Upload** tab.
2. Select **CA Bundles** as **Type**.
3. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
4. Select the root certificate by using the **Choose File** button to find the certificate **Filename**.
5. Select **Upload**.  
You should receive a success message.

#### **Upload the Intermediate CRL**

1. Select **Certificate Revocation List** as **Type**.
2. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
3. Select the intermediate CRL by using the **Choose File** button to find the intermediate CRL **Filename**.
4. Select **Upload**.



You should receive a success message with details about the CRL source.

### ***Upload the Intermediate Certificate***

1. Select **Intermediate Certificate** as **Type**.
2. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
3. Select the intermediate certificate by using the **Choose File** button to find the intermediate certificate **Filename**.
4. Select **Upload**.  
You should receive a success message.

### ***Upload the Device CRL***

1. Select **Certificate Revocation List** as **Type**.
2. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
3. Select the device CRL by using the **Choose File** button to find the device CRL **Filename**.
4. Select **Upload**.  
You should receive a success message with details about the CRL source.

### ***Upload the Device Certificate***

1. If you generated the initial CSR on another appliance, you have to concatenate your private key with the certificate that you received. See [Install Certificates in a Cluster](#) for instructions. The resulting combination file would be uploaded as **Type of Certificate with Private Key**.
2. Otherwise, select **Certificate** as **Type**.
3. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
4. Select the device certificate by using the **Choose File** button to find the certificate **Filename**.
5. Use **Destination Filename** to change the filename of the certificate. This field can be left blank if the name stays the same.  
If Privileged Access Manager generated the CSR, the "Destination Filename" must match the name of the CSR to match the private key properly. Rename the certificate that is received from the third party if necessary, so that:
  - a. Its base name is the same as the one that originally generated.
  - b. Its extension is ".crt".
 For example, if the original PEM name was abc.pem, the uploaded file must be named abc.crt.
6. If you are uploading a Certificate with a Private Key, enter the **Passphrase** that you used to create the Key, then re-enter it in **Confirm**.
7. Select **Upload**.  
You should receive a success message.

### **Verify and Set the Certificates**

Once all the required files have been uploaded, you inspect the files, verify them, and accept them. Once you accept the certificate chain, the appliance asks you to reboot. The certificate partially takes effect upon acceptance of the new certificate. We recommend applying certificates while the appliance is in maintenance mode, and to reboot the appliance before disabling maintenance mode.

#### **Follow these steps:**

1. On the **Download** tab of the **Security** page, select the **Filename** field and inspect the drop-down list of files. All the certificate and CRLs should be listed. Default files are also in the list.
2. On the **Set tab**, select the certificate that was generated by the third-party CA.
3. Select **Verify** to ensure that Privileged Access Manager accepts the certificate.  
Either a confirmation phrase or error message is provided at the top of the page.  
A success message means that the entire certification chain is valid.
4. After the verification, select **Accept** to apply the new certificate.  
The appliance asks you to reboot. The certificate does not take effect until the appliance is rebooted.



5. To activate the new certificate, select the **Reboot** button to reboot Privileged Access Manager.
6. After the reboot, logging in to the PAM server should not present an invalid certificate icon or message. On the **Set** tab of the **Configuration, Security, Certificates** page, the **System Certification** field shows the newly activated certificate name.

**NOTE**

For related information, see the following topics:

- [Secure Connections Using SSL Certificates](#)
- [Extract Required Certificates and CRLs from a Single SSL Certificate](#)
- [Certificate Revocation Update Options](#)
- [Sign Java Applets](#)
- [Delete a Certificate, CA Bundle, or CRL](#)

## Obtain and Apply SSL Certificates for a Production Cluster

This content describes how to obtain and apply SSL certificates from an in-house or third-party CA for a production cluster.

**NOTE**

To obtain and install SSL certificates for a single-server production environment, see [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#).

To create and install a self-signed SSL certificate for a small development environment, see [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#).

To secure communication between PAM servers and user sessions in a clustered environment, each node in the cluster requires the *same* SSL certificate that contains the FQDN and IP address of the VIP and every member of the cluster.

**IMPORTANT**

You do *not* need to stop the cluster to install certificates; install them one node at a time with the cluster up.

Do the following procedures in order to obtain a certificate from a Certificate Authority (CA) and apply it to all the nodes in your cluster:

### **Create a Certificate Signing Request (CSR) and Send it to the CA**

Designate any node in the Primary Site *other than the master* as the *CSR Originator* for the whole cluster and create the CSR from that server.

#### **Follow this procedure on the CSR Originator:**

1. On the **Create** tab of the **Certificates** page, select the **CSR** option for **Type**. Enter information for the following fields. Do not use special characters.

- **Key Size:** We recommend 2048 bits. 4096 bits is more secure, but it slows down TLS handshakes and increases processor load during handshakes.
- **Common Name:** Enter the FQDN of the cluster Virtual IP address, such as `pam.ca.com`. This field maps to the CN field of the X.509 certificate.
- **Country:** Enter the two-letter country code, such as US, FR, or JP. This field maps to C value of the X.509 certificate.
- **State:** Enter the optional State or Province, such as Illinois, or Quebec. This field maps to ST value of the X.509 certificate.
- **City:** Enter the optional locality or city designation, such as Paris or Islandia. This field maps to L value of the X.509 certificate.
- **Organization:** Enter the organization, typically a company, for the certificate, such as "Acme Technologies." This field maps to O value of the X.509 certificate.
- **Org. Unit:** Enter the optional organizational unit name, typically a subdivision, or location of the Organization, such as "Security BU". This field maps to the OU value/Organizational Unit designation of the X.509 certificate.
- **Days:** Days are used only for self-signed certificates.
- **Alternate Subject Names:** Enter the FQDN and IP address for the VIP and every member of the cluster. Any hostname or short VIP name that is used to access the cluster should also be added. Each FQDN, IP address, or alias should be on its own line. This list must include the **Common Name**. Do not add a newline (line feed) after the last entry. Refer to the X.509 Subject Alternative Name.
- **Filename:** Create a name for the certificate. This file name is also the name of the private key that is generated. The name must exactly match the name of the certificate when uploaded.

**TIP**

Include the creation or expiration date in the filename. For example, name it `PAM-Cluster_exp2019-07-19`.

2. Select **Create**.
3. On the **Download** tab, select the filename of the CSR you created, which has a PEM (Privacy Enhanced Mail) extension.
4. Select **Download**. Use this file to request a certificate from a Certificate Authority (CA) such as Entrust. Users do not have to install root certificates because the third party validates the site.
5. Select the Private Key (which has the same name as the CSR, but a .key extension) from the filename drop-down list. It is under the **Private Keys** heading,
6. Enter a **Password** and **Confirm Password** for encrypting the private key. Record this password for later use.
7. Select **Download**. Save the **Private Key** to add it later to the received Certificate for the other cluster members.
8. Follow the instructions provided by your CA to request the certificates using the downloaded CSR.

**IMPORTANT**

If the Certificate Authority provides all the required certificates and certificate revocation information in a single certificate file, follow the procedure described in [Extract Required Certificates and CRLs from a Single SSL Certificate](#) to extract them.

### Upload and Apply the Third-Party Certificates on the CSR Originator

Once you have the certificates and CRLs for their chain of trust, upload and apply them on the primary site node where you generated the CSR.

#### **Upload the certificates in the following order to avoid errors:**

1. **Upload the Root Certificate:**
  - a. Go to the **Configuration, Security, Certificates** page. Select the **Upload** tab.
  - b. Select **CA Bundles** as **Type**.
  - c. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - d. Select the root certificate by using the **Choose File** button to find the certificate filename.

- e. Select **Upload**.  
If the operation completed, a success message appears at the top of the screen.
2. **Upload the Intermediate CRL:**
  - a. Select **Certificate Revocation List** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
  - c. Select the intermediate CRL by using the **Choose File** button to find the intermediate CRL filename.
  - d. Select **Upload**.  
If the operation was successful, a message appears at the top of the screen with details about the CRL source.
3. **Upload the Intermediate Certificate:**
  - a. Select **Intermediate Certificate** as the **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - c. Select the intermediate certificate by using the **Choose File** button to find the intermediate certificate filename.
  - d. Select **Upload**.  
If the operation was successful, a message appears at the top of the screen with details about the intermediate certificate.
4. **Upload the Device CRL:**
  - a. Select **Certificate Revocation List** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
  - c. Select the device CRL by using the **Choose File** button to find the device CRL filename.
  - d. Select **Upload**.  
If the operation was successful, a message appears at the top of the screen with details about the CRL source.
5. **Upload the Device Certificate:**
  - a. Select **Certificate** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - c. Select the device certificate by using the **Choose File** button to find the certificate filename.
  - d. Use **Destination Filename** to change the filename of the certificate. This field can be left blank if the name stays the same.  
If Privileged Access Manager generated the CSR, the "Destination Filename" must match the name of the CSR to match the private key properly. Rename the certificate that is received from the third party if necessary, so that:
    - a. Its base name is the same as the one that originally generated.
    - b. Its extension is ".crt".
For example, if the original PEM name was abc.pem, the uploaded file must be named abc.crt.
  - e. If you are uploading a Certificate with a Private Key, enter the **Passphrase** that you used to create the Key, then re-enter it in **Confirm**.
  - f. Select **Upload**.  
If the operation completed, a success message appears at the top of the screen.
  - g. Select **Verify** to ensure that Privileged Access Manager accepts the certificate.  
Either a confirmation or an error message is provided at the top of the page.
  - h. Do **not** accept the certificates until all the cluster members have uploaded their certificates. Setting the accepted certificates requires a reboot. Wait until you complete the next procedure for other cluster members before turning off the cluster and accepting certificates on each member.

### **Verify and Apply the Certificates on the CSR Originator**

Do the following procedure on the primary site node where you generated the CSR to verify and apply the certificates. **Follow these steps:**

#### **Follow these steps:**

1. Turn on Maintenance Mode to prevent new logins:
  - a. Navigate to **Configuration, Diagnostic, System**.

- b. Set the **Maintenance Mode** option to **On**.
  - c. (Optional) Monitor the server until all user sessions have ended to avoid abruptly terminating any active user sessions by stopping PAM prematurely.
2. Navigate to the **Configuration, Certificates** screen and select the **Download** tab.
3. Select the **Filename** field and inspect the drop-down list of files. All the certificate and CRLs should be listed. Default files are also in the list.
4. On the **Set** tab, select the certificate that was generated by the third-party CA.
5. Select **Verify** to ensure that Privileged Access Manager accepts the certificate. Either a confirmation or an error message is provided at the top of the page. A success message means that the entire certification chain is valid.
6. After verification, select **Accept** to apply the new certificate. A dialog appears stating that the system certificate has been changed and asking you to "stop the cluster and reboot the appliance to make the new certificate take effect." However, to maintain availability in a production environment, **you can proceed without stopping the cluster**. Select the **OK** button to dismiss the dialog. Do **not stop** the cluster.
7. Do the following steps to activate the new certificate by rebooting the server:
  - a. Navigate to **Configuration, Power**.
  - b. The **Power** screen displays a "Cluster Warning" stating that the PAM cluster must be turned off before powering down or rebooting any cluster member. However, since the cluster does not have to be stopped to install certificates, select the option acknowledging that you have read that guidance as shown in the following screen

I acknowledge that I have read the above guidance. (You will not be able to power off or reboot without first accepting this acknowledgment.)



capture:

- c. Select the **Reboot Instance** button. The server reboots.
8. After the reboot, do the following steps to verify that the certificate was installed correctly:
  - a. Log in to the PAM server. The PAM UI should not present an invalid certificate icon or message.
  - b. Navigate to the **Set** tab of the **Configuration, Security, Certificates** screen and verify that the **System Certification** field shows the newly activated certificate name.

### Prepare a Certificate File for Other Nodes

The certificate that is provided by the CA is only valid on the CSR Originator. For other nodes, you require a file that includes the contents of the following files that are located on the originating node:

- The private key (.key) file generated when creating the CSR.
- The certificate (.crt) file that is provided by the CA in response to the CSR.

The resulting privacy enhanced mail (.pem) file is valid for all other cluster nodes.

To combine (concatenate) the files, enter one of the following commands at a command prompt on the node where you generated the CSR:

- **Linux:** `cat private_key_file.key certificate_file.crt > combined_pem_file.pem`
- **Windows:** `type private_key_file.key certificate_file.crt > combined_pem_file.pem`

The contents of the resulting .pem file should resemble the following example:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-256-CBC, 58B125ACF0792928BA28D7BC53901D86
FiRlgSddsYYDVQ7CCI0/gqC7Llmzct8GnzhmQ+47CNXkoosE4B3EWG25o3S/skaF
QUAF8hdMHo0GapDpPyAspAjfUa2+ZPrKeRbISYyn4JIn3wKduhfqziJR2vzZwQFL
l+cKhCv3aSkh+3/ZqR5+puDWjbgfprsR5F9XPjjqKJLrdmt3qxaSjzkoQNLi7Xfpr
So35vADIJt9nP0jJ3tGAtVthMR1yaJaG1B71GkqShJ+X7o0np/Y7V14EXaV6WTrA
uRia8YETRD1BcFBxj7VEfyiI+/1x4qx1CglWAJz4oLlmp1EglWX/q8EeTz0TXduY
ADrtffYGHjzoSOjWZjLKSa3zAYo0dLgKpiToNNm2JGipHMg8jnmgtg9di52AOwqwr
266oqOaRnQ50ShpJOyxpmPgbbalSekdZzdHFiWaQCg58coQnm6kSdPGwROp3g+L
```

```

10HWKoQJMVshJZn5hn7YepD0x01aiiKCxxKkziYtY4jdbQaN0m2FmTz1xrt2AsRH
OAYgXfbKOM2FfGHAFmsWR++edch77+sc4uY+1B/NuB/gvHKtADwIGC7BLlEtaQEF
aRp1P5Nu1JEX1EVfAHjv36IOUsVDpnM9jHs981G8oBefWS/Ca6QVE6hPPlaTd8i1
JuAF08jsxT18OWIU6K/J2d53WD2zqDpIhuo5SwQQFSyKUo1e0dArpYVxpuPFHXxT
uhZgxN+pKG9KYMjtvkUqpD1rS7eXqwoK2buR2Z9LUGZ7uFFZzF5+41w+/G1SkmF9
ND+YdIlrxdni+MnGyuRdJvWjR9rM6Z2ob7/FoXqeCOwAoJCyzucWWcHH+2oItBf6
TwmcdEfVq7dEOJdu9QdgrYR2oEDm22DTbEqSDCbT+J+GNAY1UPWTHjugJ2vjwW4D
6VGQhXa5Hiipmz4FmR43gV1EKUGvSAtXHyLznp/BDHm9KdoagBINUK3U130hMOPw
3Me91epgruKLHUMs07CCqHbkkglDNCAKWlPpgQFXhqEH9dnfAbWZROxN2ekms66
RzB7+/QsGHKN7E7Z5CiUp7snKs+6NNgRdJeWbDZtmXJiAH/j4CKNNwIhYOaPN4Ox
hS6ySqkZpm5NKNmDh21KM6VZsq2JU/jnXPfSqqqvurFKgUDHvW7YvzwcG8h9ZQXu
fo3wz1z8p0ukpBro2MIPZiHfdZZCmlFPzpv1PeCvtyhaHLJs4AivWV7cxhWNsyb
KxCM9KASv4+5zNgqS2sPOIiu+QMFvobkkHliTowPHLBefattET0+ljQWivBW4B/4
j9wgrxTpTQ5Kv2Mf5XAhLXdCAhYWL5OyxsrXQY5MkcNuXY+AIaUMVt/HSaQsjYLD
v5R830SnhyeeJy71HaBjNyF8DqwhTMrEuDVkSGRyynEaUTK2uqUalLZUZSvPrZc4
+g3zW9ppjCbqoBLorWk4q9G2j3LaHoXysnxjgCWt41GHElBAenphb4zahU+dMj2
LlwJprw0adcLsw/p6ck0/IySLGJtjum4qRfQQPnD6pZQ+WjkyFZJqVDM8San01ie
dJ6yBQ1PJAspJLQNHHTG6TCZUcO93agKNd8T3RfbMygl0xVtWvOIYk5FeWz7YqIi
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFqTCCA5GgAwIBAgICEAEwDQYJKoZIhvcNAQELBQAweTELMAkGA1UEBhMCVVMx
CzAJBgNVBAGMAK5ZMREwDwYDVQQKDAhDQSwgSW5jLjEnMCUGA1UECwweQ0EsIElu
Yy4gQ2VydG1maWNhdGUGuQXV0aG9yaXR5MSEwHwYDVQQDDbDQSwgSW5jLiBJbnRl
cm1lZG1hdGUGuQ0EwHhcnMTGwNjI4MjAwMzA0WmcNMTkwNzA4MjAwMzA0WjBiMQsw
CQYDVQQGEwJVUzERMA8GA1UECAwISWxsaw5vaXNxdjAMBgNVBACMBUxpc2x1MRgw
FgYDVQQKDA9DQSBUBWZWNobm9sb2dpZXNxFjAUBgNVBAMMDTEwLjI0Mi4zOS4xNzMw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCDCnmC1HMr6WQN84dSk7+2
WFzA+FPt1WADKGS1Kz/wdc4kyVEvhzEV6u2CwndY6ORWioTkcerLnUmJ1/wQ8ojO
qHmVc1GcTT0Uic7sNtKGoh/wYDK/x6N8Gtj8TWDZ9YOb/UYG4OHe2vvdP+esB29W
zls+49+bwdSm//9NO6B72c/DGv80J9KIhUW1JK+B1nHlztivnxWJezLq6NiP9jQ+
xFNv8MECsY9cVhmIJMT5cluc5cojFcFY2+5aQzIRwrcux61t2L/CwHF5tQ1htbN3
JnjcdGt1XhEd2cz24T00tQGbxE1A4z4/rNC25CrF6TixoiFe68cqFnA0XEuK6qHv
AgMBAAGjggFQMIIBTDAJBgNVHRMEAIAAMBEGCWCsAGG+EIBAQQEAWIGQDAzBg1g
hkgBhvhCAQ0EJhYkt3B1blNTTCBHZW51cmF0ZWQGU2VydMvYIENlcnRpZmljYXRl
MB0GA1UdDgQWBBrAmPBYA2gE++tvcLcmK+2H01LQATCBsgYDVR0jBIGqMIGngBR0
SZjZFHl//vqS70zxAAk6X4dx1KGBiqSBhzCBhDELMakGA1UEBhMCVVMxMzAJBgNV
BAGMAK5ZMREwDwYDVQQHDAhJc2xhbWpYTERMA8GA1UECgwIQ0EsIEluYy4xJzA1
BgNVBASMHkNBLCBjbmMuIENlcnRpZmljYXRlIEF1dGhvcml0eTEZMBcGA1UEAwwQ
Q0EsIEluYy4gUm9vdCBDQYICEAAwDgYDVR0PAAQH/BAQDAgWgMBMGA1UdJQQMMAoG
CCsGAQUFBwMBMA0GCSqGSIb3DQEBCUAA4ICAQB10cR5k7fBrF+kTU5YE8Lc48aX
pQ9ybax2chJLfSdHUS1G+qldTatPhWqrKZsCYX7RA07+BB8VBxPie05eIL/azGrD
Pdy7tzMm0iGm68uBe71ZW/3itXv2K1SNUEMdHTy787K+2/g8GqXC7Pdf6Nc1rIy1
98nqAPUGAUhBrgCBhtlyj+OqpLF1l6No/7o81gSkujCRxICW/fDBqRZd7HZ8WZjg
m2zfbbZhpaay2leaVdKEOXzQNaexYGF4U9II/00JuBzAS0eoszNVbuwHWP+yzPdL
Vg3Xtt4EasEV6/0izqsTpyCh9rnBVF1AFVOFWYAE+HPmJju8VeJzt7VU0EST7pA8
Okc9MUoRiyfO3g8qO7uC9DM+026ymxWat6dNy8tepkALrx12xI/oqD8zqT3BxA5R
tISVCcszTdfdmAf+4DK1EbaqeUIDG8uIuBH8kR/oX7LrLZotWL17piuqpvK3pcrB
fizdZ6/+FR5GwhOYT+VdZS0FuoVrTVE6iwm+oPO0Gu35pFhKYshV/c2Hnf5NvMPY
0XU7vV5w1G+LbY5Z8u2zioEiTG+9+uNrA/ryt8MG9Q/svHlOf2C8azUeY6Ykl3mC
te7V+qAJ/ZACWhOlP/ycy8mgGIYbyuzHXKQfaJbgmR0ygaEaeoPaQp6pXycjlpSM
O2zmSDDfvuQcWjhr4g==
-----END CERTIFICATE-----

```

## **Apply the Certificates to All Other Cluster Nodes**

Follow these steps on every cluster member other than the CSR creator.

### **NOTE**

Upload the certificate files in the specified order. Failure to do so causes errors.

**Follow these steps to upload the certificates in the correct order:**

1. **Upload the Root Certificate:**
  - a. Go to the **Configuration, Security, Certificates** page. Select the **Upload** tab.
  - b. Select **CA Bundles** as **Type**.
  - c. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - d. Select the root certificate by using the **Choose File** button to find the certificate filename.
  - e. Select **Upload**.  
If the operation completed, a success message appears at the top of the screen.
2. **Upload the Intermediate CRL:**
  - a. Select **Certificate Revocation List** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
  - c. Select the intermediate CRL by using the **Choose File** button to find the intermediate CRL filename.
  - d. Select **Upload**.  
If the operation was successful, a message appears at the top of the screen with details about the CRL source.
3. **Upload the Intermediate Certificate:**
  - a. Go to the **Configuration, Security, Certificates** page. Select the **Upload** tab.
  - b. Select **CA Bundles** as **Type**.
  - c. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - d. Select the root certificate by using the **Choose File** button to find the certificate filename.
  - e. Select **Upload**.  
If the operation completed, a success message appears at the top of the screen.
4. **Upload the Device CRL:**
  - a. Select **Certificate Revocation List** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the CRL.
  - c. Select the device CRL by using the **Choose File** button to find the device CRL filename.
  - d. Select **Upload**.  
If the operation was successful, a message appears at the top of the screen with details about the CRL source.
5. **Upload the Device Certificate with Private Key:**
  - a. Select **Certificate with Private Key** as **Type**.
  - b. For **Other Options**, select the applicable format (X509 or PKCS) for the certificate.
  - c. Select the device certificate by using the **Choose File** button to find the certificate filename.
  - d. Use **Destination Filename** to change the filename of the certificate. This field can be left blank if the name stays the same.
    - a. Its base name is the same as the one that originally generated.
    - b. Its extension is ".crt".  
For example, if the original PEM name was abc.pem, the uploaded file must be named abc.crt.
  - e. Enter the **Passphrase** that you used to create the Key, then re-enter it in **Confirm**. The Certificate with Private Key requires the password that you created when downloading the Key.
  - f. Select **Upload**.  
If the operation completed, a success message appears at the top of the screen.


### Verify and Apply the Certificates on the Other Nodes in the Cluster:

Once all the required files have been uploaded, inspect the files, verify them, and accept them. Once you accept the certificate chain, the appliance asks you to reboot. The certificate does not take effect until the appliance is rebooted.

**Follow these steps on every other node in the cluster, completing all steps before starting on the next node:**

1. Turn on Maintenance Mode to prevent new logins:
  - a. Navigate to **Configuration, Diagnostic, System**.
  - b. Set the **Maintenance Mode** option to **On**.
  - c. (Optional) Monitor the server until all user sessions have ended to avoid abruptly terminating any active user sessions by stopping PAM prematurely.
2. Navigate to the **Configuration, Certificates** screen and select the **Download** tab.
3. Select the **Filename** field and inspect the drop-down list of files. All the certificate and CRLs should be listed. Default files are also in the list.
4. On the **Set** tab, select the certificate that was generated by the third-party CA.
5. Select **Verify** to ensure that Privileged Access Manager accepts the certificate. Either a confirmation or an error message is provided at the top of the page. A success message means that the entire certification chain is valid.
6. After verification, select **Accept** to apply the new certificate. A dialog appears stating that the system certificate has been changed and asking you to "stop the cluster and reboot the appliance to make the new certificate take effect." However, to maintain availability in a production environment, **you can proceed without stopping the cluster**. Select the **OK** button to dismiss the dialog. Do **not stop** the cluster.
7. Do the following steps to activate the new certificate by rebooting the server:
  - a. Navigate to **Configuration, Power**.
  - b. The **Power** screen displays a "Cluster Warning" stating that the PAM cluster must be turned off before powering down or rebooting any cluster member. However, since you do not have to stop the cluster to install certificates, select the option acknowledging that you have read that guidance as shown in the following screen capture:
 

I acknowledge that I have read the above guidance. (You will not be able to power off or reboot without first accepting this acknowledgment).


  - c. Select the **Reboot Instance** button. The server reboots.
8. After the reboot, do the following steps to verify that the certificate was installed correctly:
  - a. Log in to the PAM server. The PAM UI should not present an invalid certificate icon or message.
  - b. Navigate to the **Set** tab of the **Configuration, Security, Certificates** screen and verify that the **System Certification** field shows the newly activated certificate name.

#### NOTE

For related information, see the following topics:

- [Secure Connections Using SSL Certificates](#)
- [Extract Required Certificates and CRLs from a Single SSL Certificate](#)
- [Certificate Revocation Update Options](#)
- [Sign Java Applets](#)
- [Delete a Certificate, CA Bundle, or CRL](#)

### Extract Required Certificates and CRLs from a Single SSL Certificate

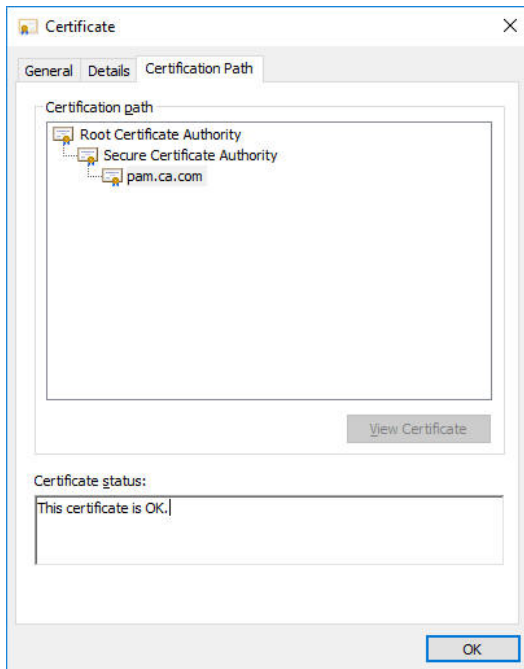
If the Certificate Authority provides all the required certificates and certificate revocation information in a single certificate file, use this procedure to extract those items from that certificate.

**Follow these steps:**

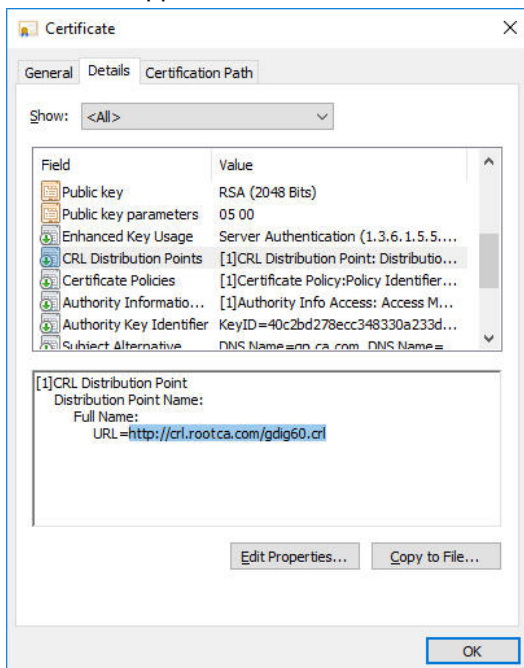
1. Copy the certificate to a convenient location on a local Windows computer.
2. In **Windows Explorer**, navigate to the location of the certificate file and open it.



A **Certificate** dialog opens.

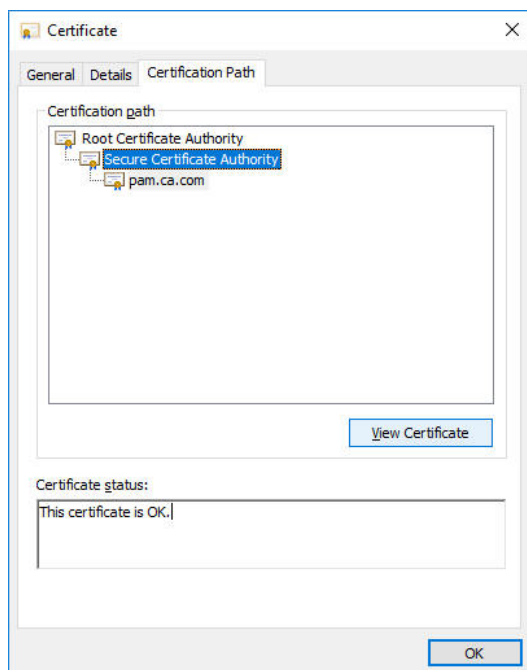


3. Select the **Certification Path** tab, where the trusted root CA is displayed at the top of the **Certification Path** pane, your device certificate at the bottom, and intermediate certificates in between.
4. Select the **Details** tab.
5. Scroll down and select the **CRL Distribution Points** field. The value appears in the window under the fields list.

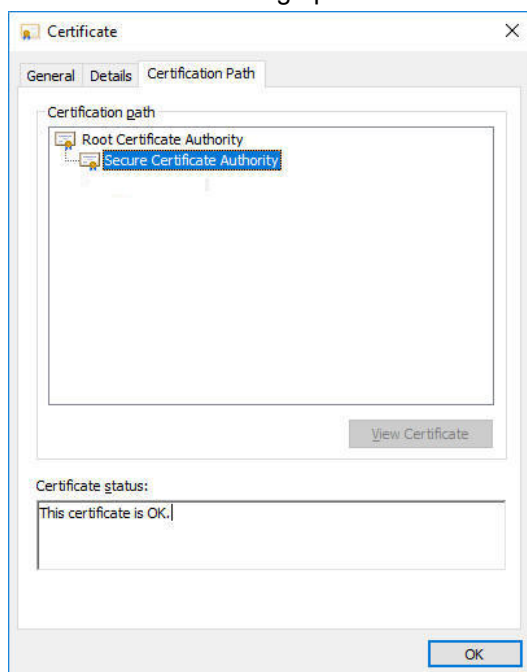


6. Select and copy the URL value.
7. Paste the URL into a browser. When prompted to open or save the CRL file, select **Save**. For convenience, save it to same location as the certificate.
8. On the **Certification Path** tab, select the intermediate certificate.

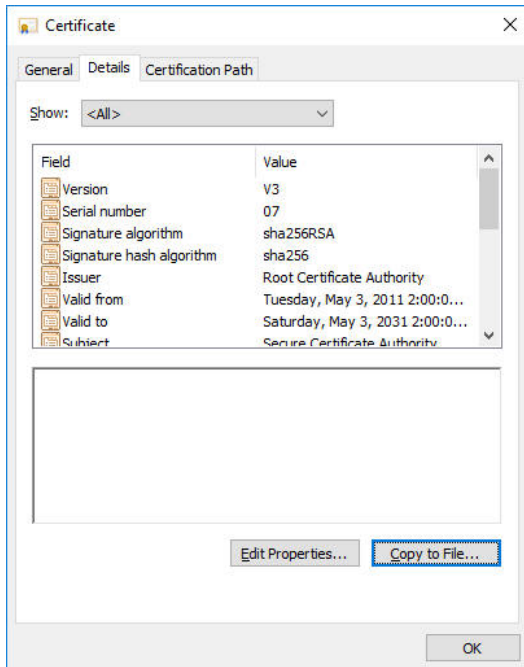




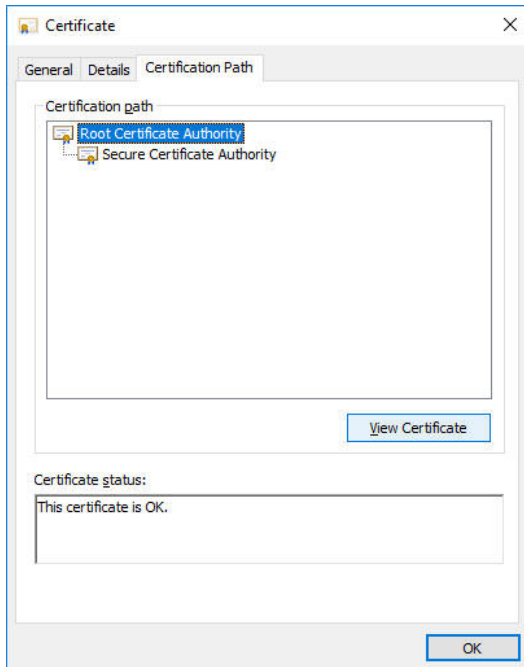
9. Select the **View Certificate** button.  
A new **Certificate** dialog opens for the intermediate certificate.



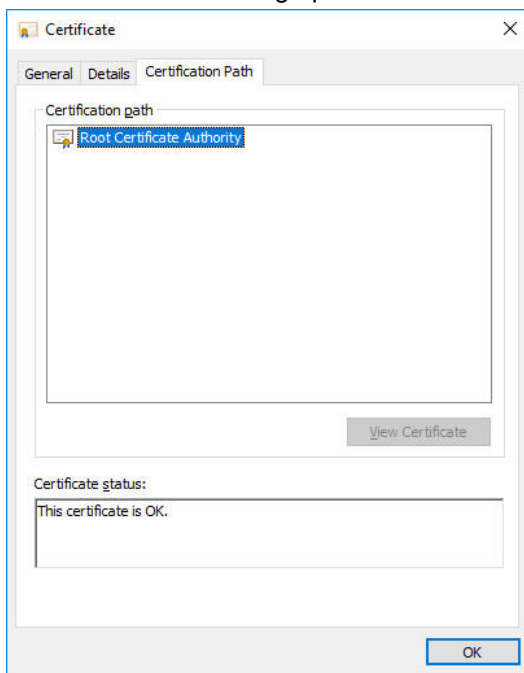
10. Select the **Details** tab on the **Certificate** dialog for the intermediate certificate.



11. Select the **Copy to File** button to save this certificate.  
The **Certificate Export Wizard** opens.
12. Follow the prompts in the wizard. For convenience, save the certificate to same location as the device certificate and CRL file.
13. Return to the open **Details** tab of the intermediate certificate dialog.
14. Scroll to the **CRL Distribution Point** field.
15. Copy the URL of the CRL Distribution Point as you did for the device certificate.
16. Paste the URL into a browser.  
When prompted to open or save the CRL file, select **Save**. For convenience, save the intermediate certificate to same location as the certificates and other CRL.
17. On the **Certification Path** tab, select the root certificate.



18. Select the **View Certificate** button.  
A new **Certificate** dialog opens for the root certificate.



19. Select the **Details** tab on the root certificate.  
20. Select the **Copy to File** button to save this certificate.  
The **Certificate Export Wizard** opens.  
21. Follow the prompts in the wizard. For convenience, save the root certificate to same location as the other certificates and CRL files.

**NOTE**

The root certificate does not have a CRL Distribution Point field.

You should now have certificate files for each level of the Certification Path, and CRLs for all but the root certificate.



root.cer



intermediat  
e.crl



intermediat  
e.cer



device.crl



device.cer



root.cer



intermediat  
e.crl



intermediat  
e.cer



device.crl



device.cer

#### NOTE

For related information, see the following topics:

- [Secure Connections Using SSL Certificates](#)
- [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#)
- [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#)
- [Obtain and Apply SSL Certificates for a Production Cluster](#)

## Certificate Revocation Update Options

Certificate Authorities revoke SSL certificates when they detect an issue with the associated identity or that the certificate key has been compromised. The CA then publishes that information so that certificate users can stop using those revoked certificates.

This content describes how to configure PAM to regularly check that its security certificate is still valid using one of the following methods:

- **Regularly downloading the latest Certificate Revocation List (CRL):** Some CAs provide *CRL Distribution Points* from which you can periodically download CRL files that contain the latest list of revoked certificates.
- **Query an Online Certificate Status Protocol (OCSP) Server (or responder):** OCSP is a dynamic alternative to CRLs. OCSP enables an application or browser to query the Certificate Authority for the revocation status of a certificate each time a connection is established.

### NOTE

If your certificate is revoked, request a new certificate from the CA and apply it to all of your PAM servers.

Topics in this content:

- [Obtain CRL Distribution Point and OCSP Server Information From a Certificate](#)
- [Manually or Automatically Download CRLs](#)
- [Obtain Revoked Certificate Information from an OCSP Server](#)
- [Route OCSP Requests Through a Proxy Server](#)
- [Configure What to Do If Certificate Revocation Information Is Unavailable](#)
- [View CRL Information](#)

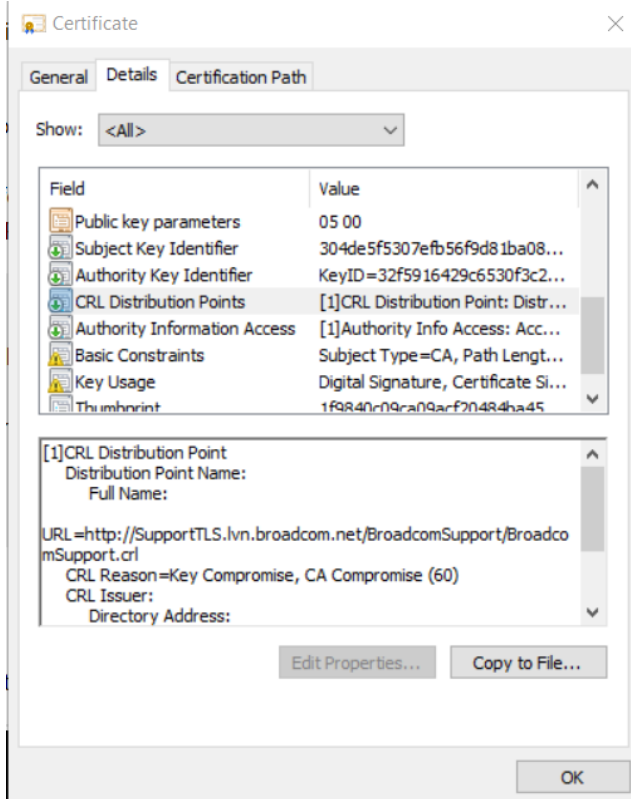
### Obtain CRL Distribution Point and OCSP Server Information From a Certificate

If necessary, use this procedure to obtain CRL Distribution Point or OCSP server information from the Certificate properties.

#### ***Obtain Information From a Certificate on Windows***

##### **Follow these steps:**

1. in Windows Explorer, navigate to the certificate file and open it.  
A **Certificate** dialog opens.
2. Select the **Details** tab.
3. To find details of available **CRL Distribution Points**, select the corresponding entry in the top list and take note of the URL or URLs in the lower panel.



4. To find out if the CA provides an OCSP server, do the following steps:
  - a. Select the **Authority Information Access** entry in the top panel.
  - b. Note whether a URL is provided in the lower panel. You do not need to copy the URL.

### Obtain Information From a Certificate on UNIX

To obtain information from a certificate on a UNIX system, enter the following command:

```
openssl x509 -in certificate_file.cer -text
```

### Manually or Automatically Download CRLs

Use one of the following procedures if your CA requires you to obtain revoked certificate information from CRLs that you download from a CRL Distribution Point.

#### Upload CRLs That You Manually Download from the CA

Use this procedure if your CA requires you to download CRLs from a CRL Distribution Point but your security protocols do not allow you to do so automatically.

#### Follow these steps:

1. Log in to the PAM UI.
2. Navigate to the **Configuration, Security, Certificates** pane and select the **CRL Options** tab.
3. For **Type**, select **Use CRL**.
4. For **CRL Type**, select **Manually Download CRLs**.
5. Download the CRL file from the CRL Distribution Point and, if necessary, copy it to the local drive of your PAM server.
6. Select the **Upload** tab and do the following steps:
  - a. Select **Certificate Revocation List** as **Type**.
  - b. For **Other Options**, select the applicable format (**X509** or **PKCS**) for the CRL.

- c. Select the device CRL by using the **Choose File** button to find the device CRL **Filename**.
- d. Select **Upload**.

You should receive a success message with details about the CRL source.

7. Return to the **CRL Options** tab.
8. Optionally, [change what action to take when revocation information is unavailable](#). The default action is **Allow User Access**.
9. Select the **Update** button.

### ***Automatically Download the Latest CRL***

Use this procedure to automatically download the latest CRL from a CRL Distribution Point.

#### **Follow these steps:**

1. Log in to the PAM UI.
2. On the **Configuration, Security, Certificates** page, select the **CRL Options** tab.
3. For **Type**, select **Use CRL**.
4. For **CRL Type**, select **Automatically Download CRLs**.
5. In the **URLs** text box, enter one or more URLs for CRL servers, one per line.
6. For **Time**, select a frequency for checking the CRL server. The default is five minutes.
7. Optionally, [change what action to take when revocation information is unavailable](#). The default action is **Allow User Access**.
8. Select the **Update** button.

### **Obtain Revoked Certificate Information from an OCSP Server**

Use this procedure if your CA requires you to query an OCSP server for revoked certificates.

#### **Follow these steps:**

1. Log in to the PAM UI.
2. On the **Configuration, Security, Certificates** page, select the **CRL Options** tab.
3. For **Type**, select **Use OCSP**.
4. Optionally, [change what action to take when revocation information is unavailable](#). The default action is **Allow User Access**.
5. [If necessary, configure the properties of a proxy server](#).
6. Optionally, specify a non-default timeout value for OCSP responses in the **OCSP Timeout** field. The default value is 10 seconds.

#### **IMPORTANT**

It is important to be aware of the following information when configuring the **OCSP Timeout** value for your environment:

- The preset timeout for most PAM UI operations (such as opening a pane or committing changes) is 60 seconds, after which a "Communication failure" error message occurs.
- The OCSP timeout applies to every certificate in your certificate chain, and the timeout value is cumulative, such that:

$$\text{Max OCSP Response Duration} = \text{Certificate Chain Length} * \text{OCSP Timeout}$$

Therefore, if your certificate chain length is four, setting the OCSP timeout to 20 seconds allows responses to OCSP queries to take up to 80 seconds. Since this duration is greater than the 60 seconds allowed for PAM UI operations, user operations may fail with a "Communication failure" error message.

7. Select the **Update** button.

The appliance automatically contacts the OCSP server regarding the specific certificate when it is used.

## Route OCSP Requests Through a Proxy Server

This procedure describes how to configure the information required if your environment requires a proxy Server to route OCSP requests and responses.

### Follow these steps:

1. Log in to the PAM UI.
2. Certificates pane **Configuration, Security, Certificates**, select the **CRL Options** tab.
3. For **Type**, select **Use OCSP**.
4. Configure the following properties of the OCSP proxy server:
  - **OCSP Proxy Server**: Specify the FQDN or IP address of the proxy server.
  - **OCSP Proxy Port**: Specify the port number to access the proxy server.

## Configure What to Do If Certificate Revocation Information Is Unavailable

The **When Revocation Information is Unavailable** option is available whether you download CRLs automatically, manually, or you use OCSP.

To use **When Revocation Information is Unavailable**, select an option from the drop-down list to determine whether a user with the certificate has access to PAM. The default is **Allow User Access**. With this mode, a user with the certificate is allowed access to PAM even though the revocation information that is related to that certificate is unavailable or not accessible. The other mode is **Deny User Access**. This mode denies access to PAM when revocation information is unavailable or not accessible.

The following table describes different conditions and the behavior that is associated with them when the **Allow User Access** or **Deny User Access** option is selected:

Condition	Deny User Access (Security Safe Mode)	Allow User Access (Operationally Safe Mode)	Co
Expired Certificate	N/A	N/A	Au
Self-Signed V3 X509 Certificate	N/A	N/A	Au
Expired CA	N/A	N/A	Au
Revoked CA	N/A	N/A	Au
CRL present, but the list is empty.	N/A	N/A	Au
No CRL present for the issuer of the certificate.	Certificate authentication fails. A CRL must be present and can be with an empty revocation list.	Certificate authentication succeeds.	
CRL expired for the issuer of the certificate.	Certificate authentication fails immediately. No checks are made to determine if the certificate is in the revocation list.	Certificate authentication proceeds and checks are made to determine if the certificate is in the revocation list. If found in the list, the certificate authentication fails or else succeeds.	
Automatic CRL download fails.	Certificate authentication fails for the URLs that failed to download as CRLs associated with the URL that failed are cleaned up. (Equivalent to <b>No CRL present for the issuer of the cert</b> condition.)	Certificate authentication succeeds or fails, depending on the existing CRL information. If the automatic download fails, no CRLs are cleaned up.	
No OCSP URI information available in the certificate	Certificate authentication fails. OCSP URI information must be present in the certificate and in all the certificates in the certificate chain.	Certificate authentication succeeds.	



Cannot connect to OCSP URI.	Certificate authentication fails.	Certificate authentication succeeds.	
-----------------------------	-----------------------------------	--------------------------------------	--

### View CRL Information

To view configured Certificate Revocation List (CRL) files and their associated status, select the **Certificate Revocation List** tab on the **Configuration, Security, Certificates** page.

#### NOTE

This option only appears if smartcard authentication is enabled for use with CRLs.

When populated with CRLs, the **Certificate Revocation List** tab displays the following fields for each certificate:

- **Issuer**
- **Next Update** (or note when it Expired)
- **Status**  
S = Stable, P = Processing, D = Downloading, I = Initial, F = Fail
- **File Name** (if applicable)
- **Distribution Point** (optional)
- **Fail Reason**  
If a CRL failure produces an error message, it is shown here.  
For example: `There is an invalid CRL file: filename`

#### NOTE

For related information, see the following topics:

- [Secure Connections Using SSL Certificates](#)
- [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#)
- [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#)
- [Obtain and Apply SSL Certificates for a Production Cluster](#)

## Sign Java Applets

Use the **Sign Applets** tab on the **Configuration, Security, Certificates** screen to sign Java Applet JARs with a certificate. For more information about signing Java applets, see [Managing Java on Your Client Workstation](#).

## Delete a Certificate, CA Bundle, or CRL

This content describes how to delete a certificate, CA bundle or CRL.

### Follow these steps:

1. On the **Configuration, Security, Certificates** page, select **Delete**.
2. Select the file name that you want to delete, and select **Delete**.

#### NOTE

For related information, see the following topics:

- [Secure Connections Using SSL Certificates](#)
- [Create a Self-Signed SSL Certificate for Use in a Testing Environment](#)
- [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#)
- [Obtain and Apply SSL Certificates for a Production Cluster](#)

## Disable and Enable Cross-Site Scripting Attack Checking

- *Reflected* cross site scripting attacks when the browser fails to do so.
- *Persisted* cross site scripting attacks: a script is persisted in the database or logs and then played back to an unsuspecting user who later logs in to Privileged Access Manager.

If Privileged Access Manager is blocking excessive events that are known *not* to be XSS attacks, disable cross site scripting attack checking. Use the controls on **Configuration, Security, Cross Site**, and contact Broadcom Support.

To identify requests that are being blocked, search the session logs for the following message:

### Disable Cross Site Scripting Attack Checking

Use this procedure to disable cross site scripting checking.

#### **Follow these steps:**

1. Log in to the Privileged Access Manager.
2. Go to **Configuration, Security, Cross Site**.
3. Select the **Disabled** option.
4. Select **Submit**.
5. Reboot the server to implement the change.

### Enable Cross Site Scripting Attack Checking

Use this procedure to enable cross site scripting checking after it has been disabled.

#### **Follow these steps:**

1. Log in to the Privileged Access Manager.
2. Go to **Configuration, Security, Cross Site**.
3. Select the **Enabled** option.
4. Select **Submit**.
5. Reboot the server to implement the change.

## Configure Enhanced Encryption for Stored Credentials

The default software encryption module that Credential Manager uses to encrypt and decrypt stored credentials is the Wolfcrypt module from WolfSSL.

### **NOTE**

If you require hardware-based encryption for stored credentials, you can configure a [Hardware Security Module \(HSM\)](#).

### **Cryptography Options**

The following cryptography options apply to:

- Inbound TLS connections
- Symmetric keys that are used for encryption and decryption of sensitive data
- Credentials that are stored in the database
- Payloads sent to the A2A clients and Windows Proxy
- One-way hash generation, such as for User passwords (using SHA512)

To protect the symmetric keys, we generate a “key wrapping” key which is unique for each deployment. The key wrapping key is automatically generated using an initial entropy seed from hardware (RDRAND; see [Cryptography Passphrase](#)) when available. This key is propagated to all cluster members.

The default software Cryptographic Provider that Credential Manager uses to encrypt and decrypt stored credentials is the Wolfcrypt module from WolfSSL.

### ***FIPS Mode for PAM***

If you have licensed and implemented FIPS Mode for PAM, the Wolfcrypt module operates in FIPS mode according to its FIPS 140-2 validation (CMVP certificate #3389). FIPS Mode has to be activated only once, and does not need to be deactivated to upgrade your appliance. See [Power, Reboot and FIPS Mode Controls](#) for information about activating FIPS Mode.

### **Cryptography Passphrase**

You do not need to enter a “primary” passphrase “seed” for cryptography. If the RDRAND hardware random number generator is available, it generates the key encryption key. RDRAND is available for physical appliances, AWS instances, and most VMware virtual machines. VMware must use virtual hardware version 9 or above (ESX 5.1), and must use EVC Mode for Ivy Bridge (or later) Intel processors. See [System Information](#) to verify whether RDRAND is available.

If RDRAND is not available, the cryptographic provider creates the manual passphrase. WolfSSL produces the passphrase using a software algorithm.

## **Configure SSH Proxy, SSH MindTerm, and TLS Cryptography Options**

Use the options on the **Configuration, Security, Cryptography** pane to configure the SSH proxy, SSH MindTerm, and TLS ciphers that are used to secure connections for accessing devices.

### **Configure SSH Proxy and SSH MindTerm Cipher Options**

Default SSH algorithms that are shown on the SSH Proxy and SSH MindTerm tabs are listed in order of priority, balancing speed with security. However, to facilitate legacy target system management, not yet updated to secure encryption algorithms, the **Cryptography** panel provides options to configure older, vulnerable KEX/Ciphers/HMAC algorithms. The risk of downgrading PAM SSH encryption should be communicated to appropriate IT administrators in your organization. This risk is due to the impact on potential breach and non-compliance to standards and legislation such as PCI DSS, FISMA, etc.

#### **WARNING**

For FIPS mode PAM, the selection of algorithms is not automatically restricted for SSH. To maintain compliance, continue to use the default algorithms.

#### **NOTE**

You can only change SSH cipher options from a PAM server that is a member of the primary site in your cluster. (The **SSH Proxy** and **SSH MindTerm** tabs are hidden on members of secondary sites.) Changes may take one minute or longer to replicate, depending on network conditions. Additionally, making changes to a standalone node, then adding a new cluster member, does not replicate the changes.

When a policy is configured to use the sftpsftplib service, it needs one of the following Hash algorithms to be enabled in SSH Proxy: hmac-sha1,hmac-sha1-96,hmac-md5

### **Follow these steps:**

1. Navigate to **Configuration, Security, Cryptography**.
2. Do the following steps on the **SSH Proxy** and **SSH MindTerm** tabs, as required:
  - a. Determine the SSH security algorithms that are appropriate for your system. By default, the **Default** option is selected. The default algorithms in each category (Cipher, Hash, Key Exchange, Compression, and Server Host

Key) are considered to provide appropriate security for SSH connections. Depending on the devices you use, you may need to define other algorithms that are not as secure.

- b. To select algorithms other than the defaults, deselect the **Default** option, and select the eye icon to the right of each text box. A window appears showing all the supported algorithms for each category. You can copy and paste the appropriate algorithms into the text box.
3. Select **Update** when you have completed your selection.

### **Enable or Disable TLS Cipher Options**

The Super, Global Admin, or Configuration administrators can disable or enable cipher suites that are used by the PAM cryptography security settings. You choose the ciphers to use by selecting **Configuration, Security, Cryptography**, and then the **TLS v1.2 Ciphers** tab.

By default, the list of ciphers you can select is determined by which type of certificate is currently configured under **Configuration, Security, Certificates**, and then the **Set** tab. For example, if your certificate uses ECDSA, the **TLS v1.2 Ciphers** tab displays selected ECDSA ciphers. Likewise, if you selected an RSA certificate, the **TLS v1.2 Ciphers** tab displays selected RSA ciphers. As an Admin, you can only select the ciphers that are supported by the certificate.

For more information on setting a certificate, see [Obtain and Apply SSL Certificates for a Single-Server Production Environment](#).

#### **NOTE**

All the cipher settings are local, and have to be set per node.

#### **Follow these steps:**

1. Select **Configuration, Security, Cryptography**, and then the **TLS v1.2 Ciphers** tab.  
The tab displays the list of ciphers. Unavailable ciphers appear grayed out. By default, the list of ciphers depends on which certificate is currently configured under **Configuration, Security, Certificates**, and then the **Set** tab.  
The **FIPS Mode** informational status field shows you whether your default filename in the **Certificates** page is in FIPS and NON FIPS mode. By default, the only cipher that is enabled in FIPS mode is **TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384**. If you require additional ciphers, you can enable them manually.
2. Select the desired ciphers.
3. Use the **Enabled Inbound TLS Ciphers** check box to select all ciphers.
4. Select **Update** to confirm and exit the **TLS v1.2 Ciphers** page.
5. After changing the cipher list, a message appears that a reboot is needed. Reboot the node. This message displays until the node is rebooted.

## **Authenticate Users Logging in to the Server**

When a user logs in to Privileged Access Manager, the server can authenticate each user locally or remotely with a third-party source.

To authenticate users locally:

1. Navigate to **Settings, Global Settings**.
2. In the **Default Auth Method** field, select **Local**.
3. Add users for local authentication from the **Users, Manage Users** page.

To authenticate users remotely using a third-party, you must configure the server to use that third-party. PAM works with the following third-party directories and devices.

- [LDAP directories](#): Compatible LDAP directory services include Microsoft Active Directory (AD), OpenLDAP, and other LDAP-compliant repositories. You can also configure [Kerberos authentication with PIV/CAC](#) for an LDAP domain.
- [LDAP+RADIUS](#): Sequential authentication from an LDAP directory and a RADIUS server
- [PKI Smart Card Authentication](#): Smart cards or a browser that is loaded with certificates for authentication.
- [RADIUS](#) and [TACACS+](#): Authentication against a RADIUS or TACACS+ server
- [RSA](#): Authentication using an RSA SecurID server
- [LDAP+RSA](#): Sequential authentication from an LDAP directory and an RSA SecurID server
- [SAML](#): SAML authentication using PAM as one or both of the following providers:
  - Identity Provider
  - Service Provider

For configuration instructions, select the authentication method you want to use from this list of supported third-party methods.

## How to Set Up LDAP Servers for User Authentication

This topic describes how to enable PAM to communicate with an LDAP server.

### Add an LDAP Device

Add a device that represents the target LDAP server, where an administrator account exists. This account must have read access to the tree from which PAM can pull administrators.

#### Follow these steps:

1. Navigate to **Devices, Manage Devices**, and select **Add**.
2. Complete the following required settings:
  - **Name**: Enter the name of the LDAP server. If Access is configured, this name is displayed on the Access page.
  - **Address**: Enter the LDAP Server IP address or fully qualified domain name. DNS must be configured on the Network Settings page for FQDN to work.
  - **Device Type**: Select Password Management. Other types can also be selected.
 Optionally, for details about other tabs on the Add Device page, see [Device Setup](#).

3. Select **Save and Add Target Applications**. The Add Target Application page opens.

4. Complete the following fields:
  - **Application Name**: Specify an application of your selection.
  - **Application Type**: Select the applicable application.
    - For Active Directory, select Active Directory or Windows Proxy. To use the Windows Proxy type, a Windows Proxy must already be set up. For instructions, see [Configure the Windows Proxy Connector](#).
    - For other LDAP servers, select LDAP.

Depending on the type, different tabs become available at the top of the Add Target Application window

5. Fill in the fields for your application type:
  - Active Directory: Enter the **Domain Name**, such as ca.com. Alter the default **Domain Controller Port** if necessary.
  - Windows Proxy: Select the Proxy from the **Available Proxies** list. Alter any other information as necessary.
  - LDAP: Select a **Server Type** of either OpenLDAP or Other. Alter the **Protocol** and **Port** if necessary. For more information about application settings, see the relevant topic:
    - [Add an LDAP Target Connector](#)
    - [Add an Active Directory Target Connector](#)
    - [Add a Windows Proxy Connector](#)
6. Select **OK** to save the application.

## Create a Target Account for the LDAP Server

Specify an application for bind requests between PAM and the LDAP server.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Accounts**, and select **Add**. The **Add Target account** pane opens.
2. Begin at the **Application Name** field. Select the LDAP application that you created previously.  
The **Host Name** and **Device Name** automatically populate.
3. In the **Account Name** field, specify an account to use for connecting to the LDAP server.
4. Enter the **Password** for this account.
5. Enter the information that is required for the application type in use:
  - Active Directory: Enter the Distinguished Name (DN). For example:  
CN=Lookup,CN=Users,DC=security,DC=com
  - Windows Proxy: Accept the default entry.
  - LDAP: Enter the DN. For example: CN=Lookup,CN=Users,DC=security,DC=com
 If necessary, alter the default **Change Process**. For more information about optional account settings, see [Add Target Accounts to Target Applications](#).
6. Select **OK** to save the account.

## Identify the LDAP Servers in Your Environment

Identify the remote LDAP server account that the appliance contacts to authenticate users. As an Administrator, you must have an account on the LDAP or Active Directory Server. This account must have read access to the tree from which you want to pull Administrators.

### Follow these steps:

1. Navigate to **Configuration, 3rd Party, LDAP**.
2. Select **Add** on the **LDAP Domains** tab.
3. Complete the following fields by searching and selecting the appropriate entries:
  - **Bind Server**
  - **Bind Application**
  - **Bind Account**
 If you have only one LDAP account, complete the Bind Account field first, then the **Bind Server** and **Bind Application** fields automatically populate.
4. For a Windows Proxy, complete the **Bind Credentials** field. For example: admin@domain.local
5. Select the appropriate **SSL Usage** value.
6. (Optional) To prevent regular synchronization updates between PAM and the LDAP directory, set the **Disable Periodic Update** option. Options related to periodic updates are disabled and you can proceed to Step 9.

#### NOTE

To perform manual updates, navigate to **Users, Manage User Groups**, and select **Refresh LDAP Groups**.

7. Set the **Sync Scope** option to specify whether to synchronize **Groups and Users** or just **Groups**.
8. Specify the **Sync Methodology** that PAM uses to synchronize with the LDAP server: **Interval** or **Schedule** then use the context-sensitive fields as described in the following procedures:
  - **Interval** (Default): Synchronize with the LDAP server at a regular interval that you specify in the **Update Interval (minutes)** field. The default value is 1440.

#### NOTE

If you set a small Update Interval value, such as 10 minutes, the high LDAP update traffic might interfere with, or disable, operation of the cluster operation. To avoid this problem, you can

manage synchronization on-demand. Navigate to **Users, Manage User Groups**, and select **Refresh LDAP Groups**.

- **Schedule:** Synchronize with the LDAP server according to a specified schedule. Scheduling allows you to avoid running the update during peak periods when PAM servers are experiencing heavy loads. In environments with multiple LDAP instances, you can also use scheduling to stagger the order and timing of refreshes for each instance.

**To configure the details of your update schedule, follow these steps**

- a. Select the **Sync Schedule** tab.
  - b. Specify how often updates should occur from the **Frequency** drop-down menu:
    - **Not Scheduled** (the default)
    - **Once**
    - **Minutes**
    - **Hourly**
    - **Daily**
    - **Weekly**
    - **Monthly**
  - c. Use the context-sensitive controls that appear to specify the schedule details:
    - **Start Time:** The start time of the refresh in hours:minutes:seconds
    - **Begin Date:** The date the refresh cycle begins
    - **End Date:** The date the refresh cycle ends (this field is optional)
    - **Reoccurs every:** The number of units specified in the Frequency attribute that should occur before the next refresh.
    - **Days** (Weekly frequency only): Select one or more days of the week on which the update should occur.
    - **Days** (Monthly frequency only): Select one or more days of the month (1 through 31) on which the update should occur.
9. To filter the LDAP members from this connection, use the fields in the **Attributes** tab.
  10. If Kerberos network authentication is set up on the LDAP server, enter the KDC server and port on the **Kerberos** tab.
  11. On the **Browse Points** tab, optionally enter one or more DN's to serve as starting points to browse the LDAP directory. A browse point becomes the root from which to start browsing the tree.
  12. To map specific fields from a PIV/CAC smart card to fields in Active Directory for authentication, use the **Custom Field Mapping** tab. We normally compare the smart card Subject Name to the DN (`distinguishedName`) AD attribute, and the Subject Alt Name on the card to the UPN (`userPrincipalName`) attribute. Use the **Subject Name** and **Subject AltName** drop-down lists to alter these mappings. For example, you might want to map **Subject AltName** to `altSecurityIdentities`.
  13. Select **OK** to save.

The newly added LDAP domain appears in the **LDAP Domains** list. Once the connection to the LDAP server has been configured, navigate to **Users, Manage User Groups**, and select **Refresh LDAP Groups** to import users.

#### **Modify the Check Down LDAP Servers Interval (Optional)**

LDAP servers can shut down or can become unavailable for other reasons. The **Check Down LDAP Servers Interval** setting specifies the interval, in minutes, when PAM checks whether a previously unavailable LDAP server has become available. The LDAP servers must be in the LDAP domains list.

#### **Follow these steps:**

1. Navigate to **Configuration, 3rd Party, LDAP**.
2. Select the **Check Down LDAP Servers Interval** tab.
3. In the **Interval (minutes)** field, set the frequency that the LDAP servers are polled. The default is 30 minutes.
4. Select **Update** to save the setting.

You can also select **Check Now** to poll all servers immediately.



### ***View Detailed Information about LDAP Activity (Optional)***

Use the **LDAP Sync History** tab to obtain detailed information about all LDAP activity, including domains and addresses, source types used (Scheduled or Manual), the exact queued times, start times, and end times, and the status of each job.

### ***Configure Multiple LDAP Servers***

You can add multiple LDAP servers for the same or different domains. Users select the correct domain during authentication. If the primary server is unavailable, the appliance connects to any backups if listed. All **Associations** and user policies will be maintained after connection to the new server.

### **Import LDAP Groups**

To import LDAP groups, use the Privileged Access Manager LDAP Browser, which launches automatically when you select an **Import LDAP Groups** button in the UI.

#### **NOTE**

You cannot import individual devices or users. To import individual objects, use the LDAP Browser to import the groups containing those objects.

When you import an LDAP group, the TLS 1.0/1.1 Connection Allowed configuration option is enforced.

To import LDAP device groups or user groups, see the following topics.

- [Import LDAP Device Groups](#)
- [Import LDAP User Group](#)

#### **NOTE**

[How to Configure Active Directory for User Authentication](#)

## **How to Configure Active Directory for User Authentication**

Active Directory is one of the LDAP directories that are used to authenticate users who attempt to access Privileged Access Manager.

### **View Records Through Cross-Domain Trusts**

If Active Directory Servers are in a cross-domain trust, you can view the user DN for a record in one Active Directory domain from a different domain. Active Directory domain trusts allow administrators to share accounts across domains. This relationship allows a domain to contain users, devices, user groups, and device groups that are *foreign* to it. The term foreign means that the directory is authoritatively maintained by a separate domain.

For each Active Directory domain that supplies users or devices, configure each domain in the UI. Navigate to configure each directory. You can then view and import these records using the PAM LDAP Browser.

#### **Follow these steps:**

1. Log in to the PAM UI as an administrator with User management privileges.
2. Navigate to **Configuration, 3rd Party, LDAP**, and configure each directory that supplies users or devices.
3. Configure the product for access to each Active Directory domain in the relevant cross-domain trust.
4. Navigate to **Users, Manage User Groups**.
5. Select **Import LDAP Groups** to launch the LDAP Browser. The LDAP Browser has a choice of cross-domain participants and any other configured LDAP directories.
6. Select one of these domains from the **Select LDAP Domain** drop-down list.
7. From the LDAP browser, select a group that contains members in this domain. Initially, the browser displays Security Identifier (SID) numbers corresponding to the entities, with no SID resolution at this point. Members that are contained



in the foreign domain are not resolved for the external domain. Members are presented relative to the current local domain.

8. To enable the cross-domain SID resolution as fully qualified DN, select **Options, Enable Group Member SID Resolution**. You can switch this setting on or off at any time.
9. Select a different browser tree item. After it has settled, return back to the previous group. The browser now builds its tree and Entry Attributes display by resolving the SIDs. This process might take a while before the Browser displays the resolved DNs for each record.
10. Select the updated menu item, **Options, Disable Group Member SID Resolution**. Move back and forth between tree items. You can see that the resolved members are cached. This cache persists while you are logged in, whether you are using the LDAP browser.

SID resolution does not affect how groups are imported into the appliance. Whether the SIDs are resolved in the LDAP browser, foreign members are resolved by the LDAP browser to create users.

### **Active Directory Password Updates**

When an Active Directory user logs in to PAM using LDAP as the authentication type, the user might be prompted to update the password. A password update is triggered when one of the following events occurs on the Active Directory Server:

- The Active Directory administrator sets the user password to a temporary value using one of the following Active Directory options:
  - New Object - User
  - Reset Password, User must change password at next login
- The user password expires

For either event, the appliance displays a User Information page with a message that the user must change the password. After the user changes the password, the old and new values are passed on to the Active Directory Server. The user is authenticated and the user record is updated. The user then gains access to the appropriate target.

The appliance updates the session logs to include password update requests. The confirmation of the record update on the Active Directory Server is also logged.

### **Configure Required LDAP Password Updates**

Configure PAM LDAP connection to use an SSL protocol.

#### **Follow these steps:**

1. Select **Configuration, 3rd Party, LDAP**.
2. Add or update an LDAP entry.
3. Enter the appropriate information for each tab.

#### **On the Add LDAP Domain tab, enter the following information:**

- Set the **SSL Usage** field to STARTTLS or LDAP

#### **NOTE**

Use a target account with sufficient privileges to reset other Active Directory users passwords.

The target account that is associated with the Active Directory Administrator must have sufficient privileges to reset the passwords of imported Active Directory users. Otherwise, the imported user cannot change a password that becomes invalid.

On the Active Directory Server, grant the minimal privileges to the account to reset passwords by issuing the following command or its UI equivalent:

```
dsacl "DN%" /I:S /G "%user_domain%\xsuiteLookup:CA;Reset Password;user"
```

- *DN* is the Distinguished Name for the domain, for example: `DC=exampledomain,DC=com`
- *user\_domain* is the short name for the Windows domain
- *xsuiteLookup* is the account Username
- Select **Disable Periodic Updates** if you do not want to update changes from the LDAP server.
- Select the **Sync Method**.
  - **Groups and Users:** Users within a group are imported as part of the group import. If Periodic Updates is enabled, LDAP changes related to Users and Groups are updated.
  - **Groups Only:** Users within a group are not imported as part of the group import. Users are provisioned the first time they login. At login time, users are assigned groups based on an LDAP lookup and the imported groups in PAM. If Periodic Updates is enabled, LDAP changes related to groups are updated. When device groups are imported, devices within the groups are also imported automatically.

**NOTE**

The following authentication types are supported for Groups Only: LDAP, LDAP + RADIUS, LDAP + RSA. When the Sync Method is Groups Only, the external API must be enabled.

- Set the **Update Interval** in minutes. Specify how often you want to update changes from the LDAP server. The Active Directory user is granted reset- password permissions and read-only permissions.

**On the Attributes tab, enter the following information:**

- Specify the **Unique Attribute**. This is the unique field in the LDAP directory that represents the user. Typically, this points to the `userName` field of the user. Example: In Active Directory, this maps to `sAMAccountName`.
- Specify the **User Group Object Class**. For Non-AD Directories, it is possible to have a custom LDAP Schema. In this schema, a non-standard objectClass is used to signify what defines a Group in the directory.
- Specify the **Group Member Attribute**. In LDAP directories, it is possible to have a nonstandard field in which the members are defined. Commonly, this is "members," but if you have a custom schema, your field may be different.
- Specify the **Group Search Filter**. If you have a large LDAP directory with many groups, you can speed up the LDAP queries by looking for groups that have a specific naming convention. Example: In the case of `PAMGroup-Admins`, refine the search to only query for "PAMGroup-".

**On the Browse Points tab, enter the following information:** If you have a large directory, set specific browse points to look for a user or group instead of traversing from the root of the directory. The browse points help to expedite the LDAP queries.

**On the Domain Trust tab, enter the following information:** Select one or more Domain Trusts from the **Available Domain Trust** list. Using the arrows, add or delete them from the **Selected Domain Trust** list.

**Configure Required LDAP Password Updates**

The **Custom Field Mapping** tab (**PIV/CAC Field**, **Subject Name**, **AltName**): Custom field mapping is used when aligning PIV/CAC authenticated users back to an LDAP Directory, such as a CA Directory or Active Directory. When looking up a CAC user, PAM uses the Subject or Subject Alternative Name (SAN) on the certificate back to the directory. In your directory, this value is stored in an Attribute on the user record within the directory. Example: The SAN of the certificate is `first.last@company.com`. This value is stored in the email field of an Active Directory user object.

**Configure LDAP and RADIUS in Combination to Authenticate Users**

Privileged Access Manager can use a combination of an LDAP server and RADIUS server to authenticate users.

**Follow these steps:**

1. Set up the LDAP server and the RADIUS server. As an example, the RADIUS server has a record for a user named **user1**.
2. Configure the appliance to use the LDAP and RADIUS servers. Servers must be available for each type.

- **RADIUS server:** See the instructions for [setting up RADIUS or TACACS+](#)
- **LDAP server:** See the instructions for [setting up LDAP](#).

When you specify the LDAP server for the appliance, set the **Unique Attribute** field to an attribute in the LDAP user record that identifies the user. The LDAP attribute that you enter must have the same value as the user name of a RADIUS user record. This common value enables the two servers to authenticate a user.

#### NOTE

For Active Directory, the LDAP attribute is typically the **sAMAccountName** or **userPrincipalName**. For other LDAP servers, it is typically **uid**. Regardless, you can use any LDAP attribute.

For example:

- RADIUS user-name: **user1**
- LDAP user record: **sAMAccountName=user1**
- Unique Attribute: **sAMAccountName**

The LDAP+RADIUS configuration is configured.

At the UI login screen, the user experience is reflected by the following steps:

1. The user enters user1 and the password.
2. For the Authentication Type field, they select **LDAP+RADIUS**.  
The **Domain** and **RADIUS Password** fields display.
3. Select the applicable LDAP Domain from the drop-down list.
4. Enter the RADIUS password for user1.

User1 is authenticated against the LDAP server. If the first authentication is successful, user1 is authenticated against the RADIUS server. If authentication is successful, user1 gets logged in to Privileged Access Manager.

## How to Configure PKI Smart Card Authentication

Privileged Access Manager can authenticate users who log in with a PKI smart card. The appliance authenticates each by the user certificate that is loaded on the smart card.

#### NOTE

FIPS mode is fully compatible with PKI smart card use, including the US DOD CAC system.

Complete the following tasks to enable smart card authentication for users logging in to PAM.

#### Watch a Video

Watch this video for a demonstration on setting up PKI smart cards:

#### Set Up OCSP or CRLs for Certificate Validation

To authenticate a user who logs in with a smart card, the appliance has to determine the revocation status of the user certificate. Configuring certificate validation is a prerequisite for enabling smart card authentication.

To validate a user certificate, set up one of the following methods:

- [Use OCSP Validation](#)
- [Use CRL Validation](#)

Each procedure explains how to upload the required certificates and then enable the user certificate validation option.

**TIP**

We recommend using certificate bundles to simplify the set-up process. If you use a certificate bundle, you do not have to upload individual certificates.

**Use OCSP Validation**

You can use Online Certificate Status Protocol (OCSP) to validate the status of a user certificate. PAM sends an OCSP request to the OCSP server to validate user certificates. The OCSP server returns the required information in the user certificate.

**To use OCSP, follow these steps:**

1. Obtain the certificate bundle or the individual certificates from the Certificate Authority (CA). If you plan to use intermediate certificates, also obtain the CRL and the intermediate certificates.
2. Navigate to **Configuration, Security, Certificates** page.
3. Select the **Upload** tab.
4. Upload the root certificate or certificate bundle for each chain to be used. The root certificate must be in the certification path of the user certificate.  
Complete the following fields then select **Upload**.
  - **Type:** Select CA Bundles (recommended) or Certificate  
To create a CA Bundle on a Windows system, use Microsoft Certificate Manager. To access the Certificate Manager, select the **Start** button. In the search field, enter **certmgr.msc**. The Certificate Manager (certmgr) opens.
  - **Other Options:** Select the format (X509 or PKCS) of the certificate you are uploading.
  - **Filename:** Browse to the root certificate or bundle on your local system that you want to upload.
  - **Destination Filename:** Optionally, change the filename of the certificate. Otherwise, leave this field blank.
  - **Passphrase:** If necessary, enter the password for the certificate.
5. Optionally, upload the CRL and any intermediate certificates. Depending on the PKI in the environment, intermediate certificates might be necessary. The certificate must be in the certification path of the user certificate.  
Complete the following settings and select **Upload**.
  - **Type:** Select Intermediate Certificate
  - **Other Options:** Select the format (X509 or PKCS) of the certificates you are uploading.
  - **Filename:** Browse to the certificate on your local system that you want to upload.
  - **Destination Filename:** Optionally, change the filename of the certificate. Otherwise, leave this field blank.
  - **Passphrase:** If necessary, enter the password for the certificate.

**TIP**

If you upload the root certificate or certificate bundle, there is no need to upload a CRL.

6. Go to the **CRL Options** tab.
7. For the **Type** setting, select **Use OCSP** then select **Update**.

**NOTE**

Next step: [Enable Smart Card Authentication](#).

**Use CRL Validation**

You can use a CRL to validate the status of a user certificate.

**To use a CRL, follow these steps:**

1. Obtain the certificate bundle or the individual certificates from the Certificate Authority (CA). If you plan to use intermediate certificates, also obtain the CRL and the intermediate certificates.
2. Navigate to **Configuration, Security, Certificates** page.
3. Select the **Upload** tab.

4. Upload the root certificate or certificate bundle for each chain to be used. The root certificate must be in the certification path of the user certificate.

Complete the following fields then select **Upload**.

- **Type:** Select CA Bundles (recommended) or Certificate  
To create a CA Bundle on a Windows system, use Microsoft Certificate Manager. To access the Certificate Manager, select the **Start** button. In the search field, enter **certmgr.msc**. The Certificate Manager (certmgr) opens.
- **Other Options:** Select the format (X509 or PKCS) of the certificates you are uploading.
- **Filename:** Browse to the root certificate or bundle on your local system that you want to upload.
- **Destination Filename:** Optionally, change the filename of the certificate. Otherwise, leave this field blank.
- **Passphrase:** If necessary, enter the password for the certificate.

5. Upload the CRL. Complete the following fields then select **Upload**:

#### TIP

If you upload the root certificate or certificate bundle, there is no need to upload a CRL.

- **Type:** Select Certificate Revocation List
  - **Other Options:** Ignore this field. The field does not apply to the CRL.
  - **Filename:** Browse to the CRL on your local system that you want to upload.
  - **Destination Filename:** Optionally, change the filename of the CRL. Otherwise, leave this field blank.
  - **Passphrase:** If necessary, enter the password for the CRL. Passwords are not typically required for CRLs.
6. Optionally, upload the intermediate certificates. Depending on the PKI in the environment, intermediate certificates might be necessary. Certificates must be in the certification path of the user certificates.

Fill out fields then select **Upload**.

- **Intermediate Certificate:** Select the intermediate certificate.
- **Other Options:** Select the format (X509 or PKCS) for the certificates.
- **Filename:** Browse to the certificate on your local system that you want to upload.
- **Destination Filename:** Optionally, change the filename of the certificate. Otherwise, leave this field blank.
- **Passphrase:** If necessary, enter the password for the certificate.

7. Go to the **CRL Options** tab.
8. For the **Type** setting, select **Use CRL**. Accept the default, Manually Upload CRLs, for the **CRL Type** setting.
9. Select **Update**.

#### NOTE

Next step: [Enable Smart Card Authentication](#).

### Enable Smart Card Authentication

After you set up certificate validation, enable smart card authentication.

#### NOTE

Linux desktops cannot use the PKI/Smart Card option. Use a Windows or Macintosh desktop.

#### Follow these steps:

1. Navigate to **Configuration, Security, Access**.
2. Select the **PKI/Smart Card Options** tab.
3. Select **Enabled** for the following options:
  - **PKI/Smart Card User Login.** This option enables smart card login. With this setting enabled, the appliance requests a user certificate during login.
  - **Enable PKI/Smart Card Option on the Login Page.** This option adds a PKI login button on the login page.

4. Optionally, you can enable the following settings:
  - **No Login Page without PKI/Smart Card** checkbox: If you select Enabled, users must have a smart card to log in. If you select Disabled, users can authenticate using a username and password or other configured authentication methods. For most situations, you can leave this option disabled. If users are unable to authenticate using smart card, the configuration page is always available using a known username and password.
  - **Policy Identifier**: Optionally, enter the identifier to the PKI policy for the certificate.
5. Select **Save**.

### **Approve Smart Card Users to Allow Logins**

The first time that a smart card user logs in to PAM, the administrator must approve the user. This requirement does not apply to preapproved users. Preapproved users are users who are added to the appliance by means, such as CSV imports, LDAP imports, or APIs. At login, an unapproved user sees an error message indicating that the certificate registration is in process. The message reflects normal operation. After an administrator approves the user, the user can reattempt to log in.

#### **NOTE**

A user might have to notify the PAM administrator to grant approval.

#### **Follow these steps to approve a smart card user:**

1. Log in to PAM as a User/Group Manager, Operational Administrator, or Global Administrator
2. Select **Users, Approve Smart Card Users**.
3. Select Approve for each smart card user. To deny the user, select Delete.
4. Select **Save**.

The user is approved.

After a successful login, the appliance displays a message requesting a certificate to validate the user identity. From a list of certificates, the user must select the certificate that is designated for smart cards use then log in. A user can determine whether the certificate is for smart card use by viewing the certificate details. From the Details tab, the **Key Usage** or **Enhanced Key Usage** field indicates whether the certificate is for smartcard login. After the user selects the correct certificate, the appliance validates it against the certificate chain. If the validation is successful, the user is prompted to enter the smart card PIN.

## **How to Configure RADIUS or TACACS+ for Authentication**

As an administrator, you can authenticate users against RADIUS and TACACS+ servers.

RADIUS and TACACS+ users are imported as user groups. When a RADIUS server is used to identify users for a User Group, the appliance first attempts to match the User Group: Groupname to the designated Attribute 25.

The users can be refreshed manually through a link that appears on the User Group page.

Complete the following tasks:

### **Prerequisites**

#### ***TACACS+ Server Support***

The appliance can work with the following software:

- tac\_plus
- Cisco Secure Access Control Server (ACS) version 4 or 5

**NOTE**

When configuring device access to Cisco, you cannot configure a unique enabled password for each Cisco device user with TACACS.

**RADIUS Server Support**

The appliance supports the PAP and CHAP authentication for RADIUS.

**WARNING**

During RADIUS authentication, if multiple user records are found with the same RADIUS login name, the login process is blocked and is deactivates all those users. An administrator explicitly enables *one* of these users.

When importing LDAP users with RADIUS authentication, all these LDAP RADIUS users are deactivated when either of the following conditions exists:

- If multiple LDAP users have the same RADIUS login name
- If any of the LDAP user login names match an existing RADIUS user in the appliance.

**Configure a Device and Target Information**

Before you configure authentication with RADIUS or TACACS+, add the server, create a target application, and set up the target account.

**Follow these steps:**

1. Navigate to **Devices, Manage Devices**, and select **Add**.
  - a. Enter a **Name**. If Access is configured, this name is displayed on the Access page.
  - b. Enter the RADIUS or TACACS+ Server IP **Address** or FQDN. DNS must be configured on the Network Settings page for FQDN to work.
  - c. Select at least the Password Management **Device Type**.
  - d. See [Device Setup](#) for details about other Device settings (optional).
2. Select **Save and Add Target Applications**.  
The Add Target Application window appears. **Host Name** and **Device Name** are populated with your Device data.
3. Specify an **Application Name**.
4. Select RADIUS/TACACS+ Secret as the **Application Type**.  
A second tab, named RADIUS/TACACS+ Secret, appears in the Add Target Application window.
  - a. Select **Type** of either RADIUS or TACACS+.
  - b. Alter the **Port** if necessary.
  - c. For more information about optional Application settings, see [Add Target Applications](#).
  - d. Select **OK**.
5. Navigate to **Credentials, Manage Targets, Accounts**, and select **Add**.
  - a. Use the Select magnifying glass icon to select the **Application Name** you created for RADIUS or TACACS+. The **Host Name** and **Device Name** are populated.
  - b. Specify an **Account Name**.
  - c. Enter the **Secret** for this account.
  - d. For more information about optional Account settings, see [Add Target Accounts and Aliases](#).
  - e. Select **OK** to save the Account.

**Add RADIUS and TACACS+ as Third-Party Servers**

After you configure the target application and target accounts for RADIUS and TACACS+, complete the setup by adding these servers as third-party servers.



Follow these steps:

1. Navigate to **Configuration, 3rd Party, RADIUS and TACACS+**.
2. Select **Add** on the **RADIUS and TACACS+ Servers** tab and do the following steps:
  - a. Use the Select magnifying glass icon for **Account** to find the RADIUS or TACACS+ account and select it. **Server** and **Application** automatically populate.
  - b. You can also start by selecting the **Server**, then **Application**, then **Account**.
3. Optionally, select the **Timeout** tab and adjust the following settings to modify RADIUS timeout parameters:
  - **Login Timeout (secs)**: Specifies the login timeout for all RADIUS server login attempts
  - **RADIUS Timeout**: Specifies the maximum time to wait for a reply from the RADIUS server
  - **RADIUS Retries**: Specifies the number of times a request will be sent before trying the next server
4. Select **OK** to save.  
The RADIUS or TACACS+ domain appears in the **RADIUS and TACACS+ Accounts** list.
5. To enable creating a User Group for RADIUS or TACACS+, log out of the appliance and log back in.
6. Navigate to **Users, Manage User Groups**, to import users from RADIUS or TACACS+.
  - a. Select **Create RADIUS Group** or **Create TACACS+ Group**.  
To locate users in a RADIUS or TACACS+ group, each group name you specify must match a corresponding group name or ID on the RADIUS or TACACS+ server. The appliance uses the configured grouping to manage users.
  - b. Enter a corresponding RADIUS or TACACS+ group name or ID as the **Group Name**.
    - All the privileges that users maintain are derived from their group. Only users with a local account or whose group matches the group name in the UI is granted access. Contact the RADIUS or TACACS+ server administrator for the group name.
    - If a RADIUS group is provisioned but the user does not exist, a shadow RADIUS user is created. The shadow user is not visible in the user management screen or the user list.

For more information about User Groups, see [Configure User Groups](#).
7. Select **OK** to save the Group.

## Configure PAM to Support RSA SecurID Authentication

You can configure PAM to work with RSA SecurID servers and enable a user to authenticate with LDAP credentials and an RSA PIN and tokencode.

### Prerequisites

PAM 4.1.5 replaced the old RSA authentication plug-in with the new RSA authentication plugin. Because the new plug-in is REST-based, the **RSA SecurID Authentication API** must be enabled on the **SecurID Authentication Manager**. For details about how to enable the **RSA SecurID Authentication API**, search for "Configure the RSA SecurID Authentication API for Authentication Agents" in the [RSA Community documentation](#).

### Register PAM as an Authenticating Device on the RSA SecureID Authentication Manager Server

Before starting with the following configuration, make sure that the RSA SecurID Authentication API is enabled on the RSA SecurID Authentication Manager. See the previous **Prerequisites** section.

After enabling **RSA SecurID Authentication API**, copy the following items from the **RSA SecurID Authentication Manager**:

- The Access ID
- The Access Key
- The configured Communication Port

To configure RSA SecurID authentication, first register PAM as an authenticating device on the RSA SecureID Authentication Manager Server.



**Follow these steps:**

1. Verify that the **Hostname** specified on the **Configuration, Network, Network Settings** screen in the PAM UI matches the Hostname that is specified in the RSA Authentication Agent entry for the PAM instance.
2. Ask the RSA SecurID administrator to register PAM as an authenticating device on the RSA SecureID Authentication Manager Server, and to provide you with `sdconf.rec` and `sdopts.rec` files. The RSA SecurID administrator generates a `sdconf.rec` file and provides it to you.
3. Do the following steps to create and configure an `sdopts.rec` file for your environment: (If you already have an `sdopts.rec` file, simply open the file and add the new lines):

**NOTE**

Make sure the `sdopts.rec` file has UNIX-style line endings. It does not support Windows line endings.

- a. Open a text editor and add the following line:

```
USESERVER=Primary_RSA_IP:Communication_Port,10
```

For example, `USESERVER=USESERVER=203.0.113:5555,10`

**NOTE**

If IPv6 has been enabled on both PAM and the RSA Authentication Manager server, use of the authentication server's IPv6 address is supported. For example,

```
USESERVER=[fd6d:8d64:af0c:1::cafe]:5555,10
```

- b. If your environment includes replicated RSA servers, add a `USESERVER` entry for each replica server, as shown in the following example code:

```
USESERVER=Replication_RSA_IP_1:Communication_Port,10
```

```
USESERVER=Replication_RSA_IP_2:Communication_Port,10
```

```
...
```

```
USESERVER=Replication_RSA_IP_n:Communication_Port,10
```

- c. Add the Access ID and Access Key collected from the RSA SecurID Authentication Manager after enabling the **RSA SecurID Authentication API**, as shown in the following text:

```
ACCESSID=64_Bit_AccessID
```

```
ACCESSKEY=64_Bit_Access_Key
```

The contents of a sample `sdopts.rec` file appears similar to the following text:

```
# RSA Servers
```

```
USESERVER=rsa-authmgr-primary.domain.com:5555,10
```

```
USESERVER=rsa-authmgr-replica-1.domain.com:5555,1
```

```
USESERVER=rsa-authmgr-replica-2.domain.com:5555,1
```

```
# Config
```

```
ACCESSID=2ba0uc767851d204v8gt7tax7sre9n2756q19d1t56210j85253h4948fhlt7o33
```

```
ACCESSKEY=z9xcd934fg4809499a1ge5m53f7srda2vv8406pr9a59s67ard22q94tsymuc4h
```

- d. Save the file as `sdopts.rec` and close the editor.
4. Do the following steps to upload the `sdconf.rec` and `sdopts.rec` files to the appliance:
  - a. Go to **Configuration, 3rd Party, RSA**.
  - b. Select the **Upload File** tab.
  - c. Select **Choose File**, locate the `sdconf.rec` file, then select **Upload**.
  - d. Select **Choose File**, locate the `sdopts.rec` file, then select **Upload**.

**NOTE**

The **Node secret** on the **RSA Files** tab is populated after the first successful user authentication.

## **Configure the RSA SecurID 800 Hybrid Authenticator**

Configure the product to allow authentication using an RSA USB token.

RSA SecurID 800 authentication requires advance preparation by the RSA SecurID administrator. Indicated in Preparation / Authentication.

## **Configure LDAP+RSA Authentication**

The product allows a user to authenticate with LDAP credentials and an RSA PIN and tokencode readout from an RSA SecurID authenticator.

### **Follow these steps:**

1. Set up the LDAP server and the RSA SecurID server. As an example, the RSA server has a record for a user named **user1**.
2. Configure the appliance to use the LDAP and RSA servers.
  - **RSA server:** See the previous instructions in this topic.
  - **LDAP server:** See the instructions for [setting up LDAP](#).

For the LDAP configuration, set the **Unique Attribute** field to an attribute in the LDAP user record that identifies the user. The LDAP attribute that you enter must have the same value as the user name of an RSA SecurID user record. This common value enables the two servers to authenticate a user.

### **NOTE**

For Active Directory, the LDAP attribute is typically the **sAMAccountName** or **userPrincipalName**. For other LDAP servers, it is typically **uid**. Regardless, you can use any LDAP attribute.

For example:

- RSA SecurID username: **user1**
  - LDAP user record: **uid=user1**
  - Unique Attribute: **uid**
3. For LDAP, use the PAM LDAP Browser to import and register the LDAP user group which contains user1. After the import, users in that group are now provisioned to apply both authentication types when logging in.

### **User Experience Example:**

1. At the UI login screen, user1 enters the user name and password
2. User 1 selects **LDAP+RSA** for the Authentication type.  
More fields appear for the LDAP and RSA servers.
3. User1 enters the following credentials:
  - LDAP Password and Domain
  - RSA Passcode (PIN+Tokencode)

User1 is authenticated against the time-sensitive RSA server. If the first authentication is successful, user1 is authenticated against the LDAP server. If authentication is successful, user1 logs in to PAM.

## **Using SAML 2.0 to Authenticate Users**

Learn how to configure PAM to use Security Assertion Markup Language (SAML) 2.0 to authenticate users.

PAM supports SAML 2.0, an XML-based open standard data format for exchanging authentication and authorization data between two entities, as an authentication option.

PAM can operate as either of the following SAML 2.0 entities for a web portal SSO connection:

- Identity Provider (**IdP**) – Authenticates a user identity and generates an assertion
- Service Provider (**SP**) – Consumes the assertion (user identity) and provides access to a service or resource.

Depending on whether PAM is the IdP or SP, SAML-compliant partners can assume the complementary role:

- **Privileged Access Manager** as an IdP handles transactions accordingly:
  - **IdP-initiated connections** – The user is provided direct access to Privileged Access Manager. During a user login, PAM authenticates the user. After login, the user is able to launch a Web Portal to the SP (AWS Management Console) without requiring authentication. The user then has access to the SP (AWS) facilities.
  - **SP-initiated connections**: The user accesses the SP directly and the SP redirects the user to Privileged Access Manager for authentication. After the user is successfully authenticated, the user is redirected back to the SP post-login landing page.
- **Privileged Access Manager** as an SP: If communication is initiated at Privileged Access Manager, any other entity can be the remote IdP, including another PAM server.

### **Next Step**

- [Configure PAM as a SAML Identity Provider \(IdP\)](#)
- [Configure PAM as a SAML Service Provider \(SP\)](#)

## **Configure PAM as a SAML Identity Provider (IdP)**

You can configure Privileged Access Manager as an Identity Provider (IdP) to provide authentication services to a SAML 2.0 Service Provider (SP). The PAM IdP supports the HTTP POST binding for sending messages.

This topic contains the instructions to configure PAM as an IdP:

### **Prerequisites for SAML Configuration**

Before you configure the appliance as an IdP, complete the following tasks:

- [Provision user accounts](#)
- [Configure SAML global settings in the PAM UI](#)
- [Obtain a certificate for signing responses](#)

### ***Provision User Accounts at Each Side***

The IdP and SP must have user accounts with matching user names. Users must have permission to access resources at the SP.

### ***Configure SAML Global Settings in the UI***

Before you configure the IdP configuration, confirm the default SAML settings.

#### **Follow these steps:**

1. Select **Settings, Global Settings**.
2. Select the **SAML** tab.
3. Verify the following two settings:
  - **Require Inherited SAML Auth**: When the authentication method for a user group is set to SAML, this option applies SAML authentication to all user group members. The appliance disregards the authentication method for each individual group member. This setting is selected by default.
  - **SAML Re-authentication Period (Minutes)**  
This setting applies only when PAM is the IdP. This setting specifies the minutes of inactivity before a session with a PAM IdP expires. A subsequent SSO request requires the user to log in again. Default: 60 minutes

### ***Obtain a Certificate to Sign Authentication Responses***

To sign and encrypt SAML responses for an SP, the PAM IdP must have a signed certificate from a Certificate Authority.

**To obtain an SSL certificate, follow these steps:**

**NOTE**

These steps apply for a single instance of PAM and for a cluster. In a cluster, complete the following procedure *only* on the first member of the primary site.

1. In the UI, navigate to **Configuration, Security, Certificates**.
2. On the **Create** page, select **CSR** (Certificate Signing Request). When you create a CSR, the appliance creates the CSR and a private key file.  
For information about completing the CSR form, see [Create a Self-Signed Certificate or a CSR](#).
3. Download the CSR and send it to the Certificate Authority.  
The Certificate Authority returns a certificate file and a CRL.
4. After you have the certificate file, go to **Configuration, Security, Certificates**.
5. Select the **Upload** page and configure the following options:
  - **Type:** Certificate
  - **Other Options:** X509
6. Select **Upload**. The certificate is now available to the appliance.  
For a cluster, you must copy the certificate and the private key to all other cluster members. For instructions, continue to the next procedure.

**Upload Key/Certificates In a Clustered environment**

In a cluster, the IdP configuration is automatically replicated across all cluster members. The certificate is not replicated. You must copy the certificate and private key from the first member of the primary site to every other cluster member.

On the first member of the primary site, **follow these steps**

1. Go to **Configuration, Security, Certificates**.
2. Go to the **Download** page and download the private key file to your local system.
3. Create a file using a text editor.
4. Into this file, copy the contents of the private key file and the certificate file from the Certificate Authority. The private key file was generated when you created the CSR.
5. Save the new file.

On *every other member* of the cluster (excluding the first member of the primary site), **follow these steps**:

1. Log in to the UI and select **Configuration, Security, Certificates**.
2. Select the **Upload** tab and set the following fields:
  - Type: Certificate with Private Key
  - Other options: PKCS
3. Select **Choose file** and select the new, combined file.
4. Select **Upload**.

**Configure PAM as an IdP**

A SAML SSO partnership is between an SP and IdP. The SP has the resources that users request while the IdP has the information to authenticate users who make the requests. The IdP returns an assertion that contains information about the user. The SP uses this information to determine whether to grant access to a user.

In a clustered environment, the appliance replicates the IdP configuration from the first member of the primary site to other members across the cluster. The exception is the key/certificate file that encrypts responses. You manually copied the key/certificate file to each member of a cluster in the [previous procedure](#).

**To configure PAM as an IdP, follow these steps:**

1. **For clustered environments only:** At the first member of the primary site, turn off the cluster. If the cluster is active, you cannot enable the IdP settings.
2. Go to **Configuration, Security, SAML, IdP Configuration** tab.

3. Complete the following settings listed:
  - **Status:** Indicates whether the IdP is enabled. Enable this setting to complete the IdP configuration.
  - **Entity ID:** Enter a unique test string to identify this IdP.
  - **Fully Qualified Hostname:** Enter *one* of the following values. Ensure you specify the fully qualified host name.
    - For a single instance, enter the value of the IdP host name, such as capam.example.com.
    - For a primary cluster member, enter the VIP address or VIP host name.

**TIP**

Inform your federation partners to use the fully qualified host name when accessing the PAM IdP.

- **Signature Algorithm:** Select the encryption algorithm to sign certificates.
  - **IdP Certificate:** Select a certificate to sign assertions. Use the default certificate, gkcert.crt, installed with PAM or a certificate that you uploaded in the [previous procedure](#).
4. Optionally, select **Download IdP metadata** to generate an XML file and send it to the remote SP.

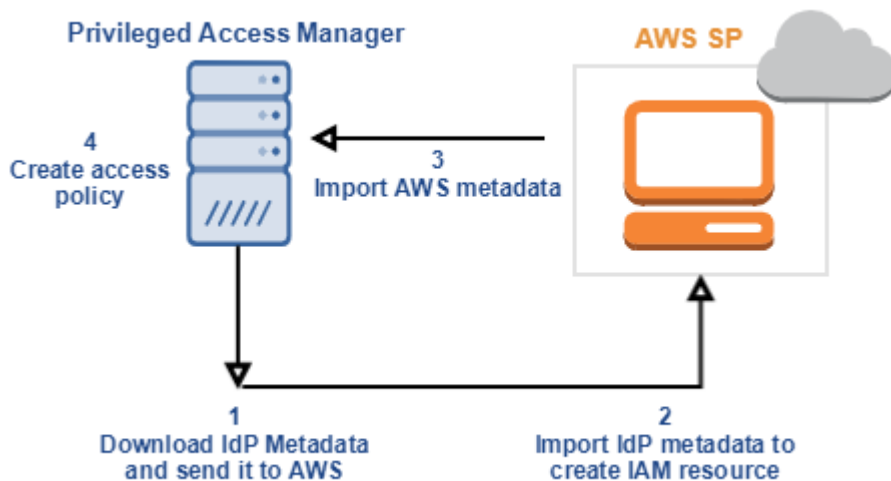
The configuration is complete. If you change any of these settings, select **Update IdP Configuration**.

For details about SAML metadata, see the [SAML specifications](#).

**Example: Configure SAML SSO to an AWS SP**

The following example shows how to set up federated SSO between a PAM IdP and Amazon Web Services (AWS) as the SP. In this example, the configuration relies on metadata. The process is reflected in the following figure:

**Figure 18: saml sso with AWS SP**



**Download IdP Metadata and Send it to the AWS SP** To establish trusted communication between the IdP and AWS SP, first configure and download the IdP metadata file. The downloaded file, named idp-metadata.xml, describes the IdP-supported SAML services. The file contains:

- Information about how an SP can send authentication requests to the IdP
- Certificate (public key) for verifying the signed assertions
- FQDN or IP address of the PAM server

**NOTE**

If you change the FQDN or the certificate changes, update the IdP metadata and resend the file to the SP.

**Follow these steps:** This procedure assumes that the IdP is already enabled.

1. Log in to the PAM UI as a Configuration Administrator.
2. Navigate to **Configuration, Security, SAML**. Select the **IdP Configuration** tab.
3. Enter values for the following fields:
  - **Entity ID:** Assign a name that identifies this IdP.  
This ID is included in the metadata file and in assertions.
  - **Fully Qualified Hostname:** Enter the fully qualified name of the IdP host. The default example is `idp.example.com`.
  - **Signature Algorithm:** Select the encryption algorithm that is used to sign the IdP certificate
  - **IdP Certificate:** Select the certificate and key you are currently using for the appliance.
4. Select **Update IdP Configuration** to apply the current certificate, host name, and your assigned ID.  
You receive a confirmation message at the top of the page.
5. Select **Download IdP Metadata** to save the `idp-metadata.xml` file locally.
6. At AWS, import the IdP metadata file, as instructed in the next procedure.

**Import IdP Metadata to Create an AWS IAM Resource** A PAM administrator sends the IdP metadata to AWS. An AWS Administrator must import the metadata file to its SP endpoint. The file provides the necessary information for AWS to make authentication requests to PAM.

#### WARNING

**CAUTION!** The following procedure describes a product that is independent of PAM.  
The procedure is provided only as an example. You might encounter different features or different appearance.

**An AWS administrator must follow these steps:**

1. Log in to the AWS Management Console and navigate to **Services, IAM, Identity Providers**.
2. Select **Create Provider** and complete the following settings:
  - **Provider Type:** Select SAML.
  - **Provider Name:** Enter a name to identify the PAM IdP.
  - **Metadata Document:** Locate the IdP metadata sent by the PAM Administrator.
3. Select **Next Step** then confirm the configuration by selecting **Create**.
4. In the left pane, select **Roles, Create New Role**.
5. Enter a **Role Name**, and select **Next Step**.
6. On the Select Role Type page:
  - a. Select **Role for Identity Provider Access**
  - b. Select **Grant Web Single Sign-On (WebSSO) access to SAML providers**
7. In the next panel, select the SAML provider that you created in the previous steps. Select **Next Step**.
8. Continue past the **Verify Role Trust** page. In this example, you do not need to edit the Verify Role Trust: Policy Document.
9. On the **Attach Policy** page, we recommend that you use select one of the pre-built policy templates, such as **Amazon EC2 Read Only Access**. If you are testing on a public EC2 instance, do not let others log in to your box. Select **Next Step**.
10. Review the confirmation then select **Create Role**. Your new role appears in the roles list.

Your AWS account is now configured to communicate with the PAM IdP. **Import AWS SP Metadata at the IdP** AWS uses the concept of roles for authentication. When the IdP generates the authentication response, the assertion must contain role data for the user being authenticated. The role definition and other information are in the AWS SP metadata. The file also includes the attributes the SP expects in the IdP

authentication response. The AWS SAML metadata file is available at: <https://signin.aws.amazon.com/static/saml-metadata.xml>. After you obtain the file, import it into PAM. **Follow these steps:**

1. Log in to the PAM UI as a Configuration Administrator.
2. Select **Services, Import SAML 2 SP Metadata**.
3. Select **Choose file** and browse to the AWS SP metadata file.
4. Select **Import SAML 2.0 SP Metadata**. A message confirms the import.  
After the import, the appliance creates two objects:
  - A web portal service. The name of the service matches the SP Entity ID in the metadata file. In this example, the service is called **AWS Management Console Single Sign-On**.
  - A device with an address of the Assertion Consumer Service at the SP.
5. Navigate to **Services, TCP/UDP Services** and select the new web portal service and update it.
6. Ensure that the Auto Login Method field is set to SAML2.0 SSO POST.
7. Select the **SAML SSO Info** tab and configure the following fields:
  - **Initiating Party**: Select **IdP-Initiated**
  - **Require Signed Authn Requests**: Clear the checkbox. The AWS SP does not send signed authentication requests.

For information about the other fields on this page, see [Configure Automatic Login to Web Portals](#).

After you complete the procedures, PAM can provide an assertion to AWS. Based on the assertion, AWS can permit access to the requested resource. **Create a Policy for Users to Access to AWS Resources** For a user to gain access to an AWS resource, set up a policy for that user at the appliance. The policy is made up of a TCP/UDP service and a device that the appliance automatically creates when you imported the SP metadata. The policy also includes selected attributes that the AWS SP accepts in the assertion response.

**Follow these steps:**

1. Log in to the PAM UI.
2. Select **Policy, Manage Policies, Add**.
3. On the **Association** panel, select a user and the device **signin.aws.amazon.com**. This device is the one automatically generated based on the SP metadata.
4. On the **Services** panel, select the **AWS Management Console Single Sign-On** service.
5. On the **SAML** panel, add the following attributes under the **Requested Attributes** column:
  - **Subject Name Identifier**: The available name identifier format is associated with the TCP/UDP service
  - **RoleSessionName**: Assign a label in the **Attribute** column. Use any identifier.
  - **RoleEntitlement**: Select Constant in the **Attribute** column. In the **Value** column, enter the concatenated AWS ARNs for the IAM role and the Identity Provider, separated by a comma. For example:

```
arn:aws:iam::123456789012:role/
MyAWSroleForMyIDP,arn:aws:iam::123456789012:saml-provider/
AWSstoredMetadataForMyIDP
```

The following picture shows an example:



Update Policy samluser - signin.aws.amazon.com

Access Services **SAML** Password Filters Recording CA PAM Server Control Transparent Login

AWS Management Console Single Sign-On

Select entries from the Requested Attribute combo box to configure additional SAML attributes. Requested Attributes in bold are required.

**+**

Requested Attribute	Name Identifier Format	Provision Type	Attribute	Value
Subject Name Identifier	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	LOCAL	User Name	
RoleEntitlement		LOCAL	Constant	arn:aws:iam:...
RoleSessionName		LOCAL	Email	

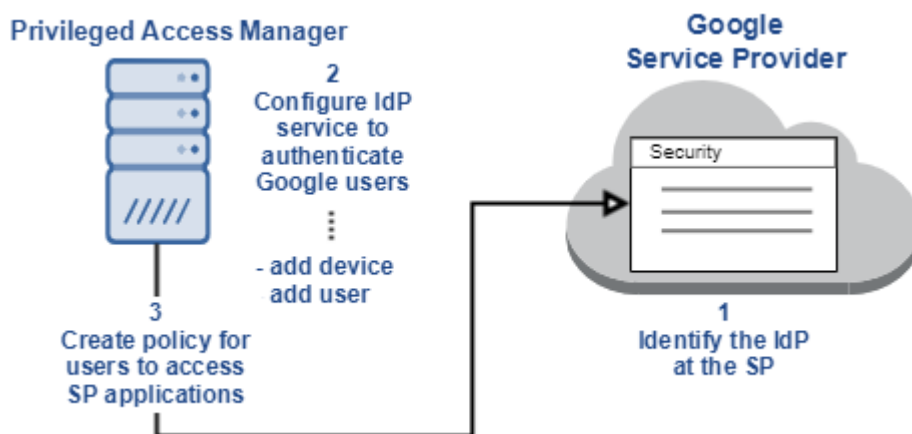
6. Select **OK** to save the policy.

The user can now access the AWS federated resource without having to log in.

### Example: Configure SAML SSO to a Google SP

You can work with an SP that does not provide metadata. In this example, PAM IdP is configured for SSO with a Google SP. Google does not use metadata to exchange information to or from its partners. The process is reflected in the following picture:

**Figure 19: SAML SSO Google Example**



**Identify the IdP at Google** At Google, the PAM IdP must be configured so it can authenticate Google accounts.

#### NOTE

The following procedure describes a product that is independent of PAM. The procedure is provided only as an example. You might encounter different features or appearance.

#### Follow these steps:

1. Log in to the Google Admin Console (<https://admin.google.com>).
2. From the main menu at the top left, select the Security, then scroll down the page and select **Set up single sign-on (SSO)**.
3. Scroll down the page and select the checkbox **Setup SSO with third party identity provider**.
4. Enter values for the following fields:



- **Sign-in page URL:** `https://capam_IP_or_hostname /idp/profile/SAML2/Redirect/SSO`
  - **Sign-out page URL:** PAM does not support single sign-out. Enter `https://capam_ip or hostname /` as a placeholder.
  - **Change password URL:** PAM does not support password changes. Enter `https://capam_ip or hostname/` as a placeholder.
  - **Verification certificate:** Upload the certificate from PAM IdP. This certificate works with the private key that is used to sign the SAML response. To obtain this certificate, take *one* of the following actions:
    - Copy the certificate from the IdP metadata file.
    - Download the certificate from the appliance. Select **PAM Configuration, Security, Certificates**, and go to the **Download** tab.
5. Select **Use a domain-specific issuer**.
  6. Optionally, to allow a specific set of users access to the application, specify entries in the **Network masks** field.
  7. Continue to the next procedure.

**Configure a Service to Authenticate Google Users** Set up a service at the IdP that represents the Google SP. No metadata is available to set up this service. Obtain the necessary information from the SP. **Follow these steps:**

1. Log in to the PAM UI.
2. Navigate to **Services, Manage TCP/UDP Services, Add**.
3. On the **Basic Info** panel, configure the settings with the following values:
  - **Service Name:** Entity ID of the Google SP. For this example, GoogleApps.
  - **Local IP:** Address of the end-user local host, such as the user laptop, in the format 127.0.0.5 (IPv4) or ::1 (IPv6). Do not use an address of an existing service.
  - **Ports:** Enter the ports of the local host, such as 443:4430.
  - **Protocol:** TCP
  - **Application Protocol:** Web Portal.
  - **Auto Login Method:** SAML2.0 SSO POST
  - **Launch URL:** URL for the ACS, using the format: `https://<Local IP>:<First Port>/a/google_domain/acs`. Enter the literal string `<Local IP>:<First Port>`. *These entries are not placeholders. Replace `google_domain` with the domain of your Google services, such as calendar or email. This domain is the location consuming SAML assertions.*
4. In the **SAML SSO Info** panel, configure the fields with the following values
  - **SAML Entity ID:** `google.com/a/google_domain`
  - **Initiating Party:** SP-initiated
  - **Require Signed Authn Requests:** Clear the checkbox.
  - **Encryption:** Select None. Google applications do not support encrypted assertions. If the SP does support encryption, you can select the **Name ID** or **Assertion** option. Then, copy the certificate from the SP in the **PEM Encryption Certificate** field.
5. On the **SAML SSO Attributes page**, select the name identifier format `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
6. Select **OK**.

**Create a Device Representing Google** Add a device that identifies the Google SP. **Follow these steps:**

1. Select **Devices, Manage Devices, Add**.
2. Most of the fields are self-explanatory, but note the following entries:

- **Address:** Enter the fully qualified domain name of the server hosting the ACS. You can extract the address from the ACS URL, for example: [https://www.google.com/a/your\\_google\\_domain/acs](https://www.google.com/a/your_google_domain/acs). The device address that is provisioned in PAM is [www.google.com](http://www.google.com).
  - **Device Type:** Access
  - **Services** tab: Select the TCP/UDP service that you configured for the SP in the previous procedure.
3. Select **OK** to save the device entry.

**Create an IdP User Matching the SP User** Create a user with a user name matching a Google user account that can log in to applications. **Follow these steps:**

1. Select **Users, Manage Users, Add**.
2. Most of the fields on the tabs are self-explanatory.
3. In the Roles panel, select the applicable user role for the user logging in to PAM simply to access the SP.
4. Select **OK** to save the user entry.

**Create a Policy for Users to Access to Google Applications** For a user to gain access to a Google application, set up a policy for that user at the appliance. The policy is made up of a TCP/UDP service, the device, and the user entry you created in the previous procedures. **Follow these steps:**

1. Log in to the PAM UI.
2. Select **Policy, Manage Policies, Add**.
3. On the **Association** panel, select a user and the device with the name **www.google.com**.
4. On the **Services** panel, select the **GoogleApps**.
5. On the **SAML** panel, add the following attribute entry: Attribute entry with the following values:
  - **Requested Attribute:** Subject Name Identifier. This attribute is always required.
  - **Name Identifier Format:** urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
  - **Attribute:** Email
6. Select **OK** to save the policy.

The user can now single sign-on to the Google application.

## **SAML SSO User Experience**

When a user makes a request, there are two types of communication flows:

- IdP-initiated: The user starts at the IdP and gets redirected to the SP.
- SP-initiated: The user begins at the SP and the SP sends an authentication request to the IdP. The IdP responds with an assertion, which identifies the user.

The two SAML SSO configuration examples illustrate each type of flow.

### ***IdP-initiated SSO to the AWS Management Console***

In the AWS example, the service you configured to the AWS Management Console is for IdP-initiated SSO.

**The SSO flow follows these steps:**

1. The user logs in to PAM and the Access page in the UI is displayed.
2. On the Access page is a link to AWS Management Console Single Sign-On.
3. The user selects the link and gains access to the Console directly without entering credentials.

### ***SP-Initiated SSO to Google Apps***

For SP-initiated communication, initiate the connection at the Google. Typically, the user has the access URL to the SP.

**WARNING**

The following procedure describes a product that is independent of PAM. The procedure is provided only as an example. You might encounter different features or appearance.

**The SSO flow follows these steps:**

1. In a browser, the user enters the URL to Google: <https://accounts.google.com/>
2. At the login, the user enters their user name.
3. The SP redirects the user to the PAM IdP.
4. If the user has not authenticated, PAM presents the login page. The user logs in and the IdP authenticates that user.
5. Following authentication, the IdP redirects the user back to Google with the assertion. The user is logged in automatically to Google.

**Configure PAM as a SAML Service Provider (SP)**

The following sections explain how to configure a PAM SP:

**Prerequisites for SAML Configuration**

Before you configure PAM to act as an SP, there are some initial tasks to complete:

- Provision user accounts
- Configure SAML Global Settings
- Obtain a Certificate to Sign Authentication Requests

These prerequisite steps are described in the next few sections.

***Provision User Accounts at Each Side***

The SP and IdP must have user accounts with matching user names. Users must have permission to access resources at the SP.

***Configure SAML Global Settings***

Before you configure the SP configuration, confirm the default SAML settings.

Follow these steps:

1. Select **Settings, Global Settings**.
2. Select the **SAML** tab.
3. Verify the following two settings:
  - **Require Inherited SAML Auth:** When the authentication method for a user group is set to SAML, selecting this option applies SAML to all user group members. The individual authentication method is disregarded. This setting is selected by default.
  - **SAML Re-authentication Period (Minutes)**  
This setting applies only when Privileged Access Manager is the IdP. This setting specifies the minutes of inactivity before a session with a PAM IdP expires. A subsequent SSO request requires the user to log in again. Default: 60 minutes

***Obtain a Certificate to Sign Authentication Requests***

A certificate for the SP is necessary to encrypt such items as an authentication request. Obtain an SSL certificate for your PAM fully qualified domain.

**Follow these steps:**

1. Navigate to **Configuration, Security, Certificates**.

2. On the **Create** tab, select **CSR (Certificate Signing Request)**. For more information, see [Create a Self-Signed Certificate or a Certificate Signing Request](#).  
Use the CSR to obtain a certificate, CA chain, and CRL from your applicable Certificate Authority.
3. After you obtain these files, upload them. Go to **Configuration, Security**, and select the **Upload** tab. Select and upload the appropriate files.
4. Go to the **Set** tab to accept the certificate.

### Example: Configuring SAML SSO with PAM

The following example illustrates how to establish SAML single sign-on between two PAM servers acting as SAML partners. In the procedures that follow:

- The SP and the IdP are both PAM appliances.
- Metadata files are used to define each partner to one another.

**Import IdP Metadata to the SP** The IdP metadata file is an XML file that describes the SAML services that the IdP provides. The document contains information about how an SP can send authentication requests to the IdP. The file contains the certificate (public key) that the IdP uses to sign all assertions. Finally, the file includes the fully qualified domain name (or IP address) of the IdP. Therefore, anytime the FQDN or the certificate changes, update the IdP metadata and upload the file to the SPs. **Download the metadata file:**

1. Log in to the PAM IdP as a Configuration Administrator.
2. Navigate to **Configuration, Security, SAML**, and select the **IdP Configuration** tab.
3. Following a change in the appliance hostname or the default certificate, update the IdP settings as follows:
  - a. In **Entity ID**, assign a unique name to identify this IdP.  
This ID gets included in the IdP metadata file and in the assertions the IdP generates.
  - b. In **Fully Qualified Hostname**, enter the value that is used for this SP, such as: mypam.example.com
  - c. From the drop-down list for **IdP Certificate**, select the certificate and private key pair.
  - d. Select **Update IdP Configuration** to apply the current certificate, hostname, and your assigned ID.
  - e. Upon changing your hostname, select **Accept IdP Certificate** in that panel.
4. Select **Download IdP Metadata** to save the metadata file locally.
5. Upload the metadata to the SP

### Upload the metadata to the SP:

1. Log in to the SP as a Configuration Administrator.
2. Navigate to **Configuration, Security, SAML, SP Configuration** tab.
3. At the minimum, complete the required fields.
4. Select **Save Configuration**.
5. Select the **Configured Remote SAML IdP** subtab.
6. Identify at least one corresponding IdP by clicking **Upload An Identity Provider Metadata**. Browse to the metadata file from the IdP and select **Upload**.
7. Move to the **Set** tab and accept the file.

The IdP is now identified by its **Friendly Name**, if available, and its **Entity ID**. **Import the SP Metadata to the IdP** This PAM SP is now aware of the IdP by way of the imported IdP metadata file. Use an SP metadata file to identify itself to the IdP. The SP and IdP now can then communicate with each other. **Download the SP metadata:**

1. If you are not already there, navigate to **Configuration, Security, SAML**, and select the **SP Configuration, Configured Remote SAML IdP** subtab.
2. Identify the line item for the IdP that you are looking for.
3. Select the **Download Metadata** link for this IdP and select it to save this SP metadata file locally.

**Upload the SP metadata to the IdP:**

1. Log in to the IdP as a Configuration Administrator.
2. Select **Services, Import SAML 2 SP Metadata** to open the import page.
  - a. **Choose File** to locate the XML file that you obtained from the SP.
  - b. Select the **Import SAML 2 SP Metadata** button to upload it to IdP.  
After you do so, you will see several acknowledgment messages. If there are errors, they are noted in red.

Uploading the SP metadata results in identification of the SP authorization function as a Service, and the SP server as a Device.
3. Confirm that a Service record has been created under **Services, Manage TCP/UDP Services**, with a **Service Name** matching the IdP SAML Entity ID. Select the **Update** button to see the details. The record has the following information:
  - Typical specifications for a Web Portal, with **Auto Login Method**="SAML2.0 SSO POST"
  - Launch URL, which is the Assertion Consumer Service URL
  - **SAML SSO Info** tab with the SAML Entity ID
  - **SAML SSO Attributes** tab with SAML SSO Subject Name Identifier Formats and SAML SSO Attributes
4. In **Devices, Manage Devices**, verify that a Device record has been created with **Name** and **Address** matching the IdP SAML-applicable FQDN.

**Provision SSO Access Policy** The SP and IdP have been configured to trust each other. Now you can provision the IdP to permit its users to access the SP services. When you open a policy for the SP (for a particular user or user group), select the corresponding SP service. The service is identified by Entity ID. This action opens the SAML tab so that its attributes can be specified.

**NOTE**

If the SAML attributes are not sufficiently identified, revise them as necessary. The SAML Name Identifier Format is initially not specified. If this value is missing, select one of the available options so that the **xAttribute** becomes available.

**SAML SSO User Experience** After you set up SAML SSO, a **Single Sign On** option becomes available on the login screen of the PAM UI. The following process assumes an SP-initiated connection:

1. The user requests a resource at the SP by selecting **Single Sign On** at the login screen.
2. The user is alerted that the login proceeds with authentication at a different target, the IdP. If there are multiple IdP targets, the user must select one from the drop-down list, then select **ENTER**.
3. The User is then brought to the login page for the IdP. No **Single Sign On** option is available at the IdP.
4. The User enters the required credentials.
5. The IdP has authenticated the user, its task is complete. Control is handed back to the SP, where the user is granted access to the application.

**JIT Provisioning**

Just-in-time (JIT) SAML provisioning in PAM enables the provisioning of new user accounts from SAML assertions.

For JIT Provisioning to work effectively, follow these guidelines:

- Create PAM user groups that match user groups that are used in the SAML assertion.
- Use the **userGroup** attribute in the assertion for these user groups.
- The user must belong to an existing user group to which the user is not provisioned, and authentication fails. The user is redirected to the login page.
- The user can belong to multiple user groups.
- If a user later logs in with a different set of user groups, the user moves to those user groups.
- Entitlements for users are defined by the user groups.
- As an administrator, you cannot manage user group membership inside the appliance. You can manage membership only using assertions.
- This user group behavior only works for users that are provisioned using JIT provisioning.

### ***JIT Provisioning User Groups Examples***

The following examples illustrate how the SAML **userGroup** attribute interacts with user groups. For these examples, the following user groups are configured in PAM: Group A, Group B, Group C, Group D.

- The SAML assertion contains Group A and Group C. The user is provisioned in those user groups
- If the assertion contains only Group E, the JIT provisioning and authentication fail. The user is redirected to the login page.
- A user belongs to Group A and Group C and the assertion contains Group B and Group D. The user account moves from Group A and Group C to Group B and Group D.

### ***Configure JIT Provisioning***

Follow the same instructions that are found in [Configure PAM as the SP](#). When you get to the **Configured Remote SAML IdP** step on the SP Configuration page, either **Upload** or **Add** the IdP information as instructed.

- If you select **Add** and you manually create an Identity Provider (IdP) record, select the **Allow Just In Time Provisioning** checkbox.
- If you select **Upload An Identity Provider Metadata** and you create an IdP record from the imported IdP metadata document, select **Update** afterwards. Select the **Allow Just In Time Provisioning** checkbox.

Select **Save Configuration**.

## **Azure AD as an Identity Provider (IdP)**

You can configure Privileged Access Manager to use Active Directory on Microsoft Azure as its Identity Provider using SAML. You can configure Azure as IdP whether Privileged Access Manager is [deployed on Azure](#) or not.

### **Set up the Azure Application**

To create an application in Azure, follow these steps:

1. Log into Azure with an account with permission to grant admin consent for API permissions.
2. In the Azure UI, select **Azure Active Directory** from the **Azure services** menu at the top of the screen (as shown highlighted in the following screen capture):

## Azure services



3. Select **App Registrations** from the **Manage** section that appears in the left rail.
4. Select **New Registration** from the menu bar on the **App registrations** pane.
5. Enter a **Name** of your choice. Do not include spaces in the name.
6. At the **Who can use this application or access this API** prompt, select one of the following options, as appropriate:
  - **Accounts in this organizational directory only (pamdev only - Single tenant)**
  - **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**
7. For **Redirect URI**, select **Web** (the default) and enter the URL of your Privileged Access Manager UI in the following format: `https://ip_address/cspm/home` . For a cluster, select the IP address of the first node at the primary site.
8. Select **Register**. The application is created.
9. Select **API permissions** from the **Manage** section in the left rail.
10. On the **Configured permissions** pane that opens, select **Add a permission**.

### NOTE

The **User.Read** delegated permission, which appears in the list of permissions is configured by default.

11. On the **Request API permissions** wizard that opens, select **Microsoft Graph**.
12. On the next page, select **Delegated permissions**.
13. Locate and open the **Directory** entry in the list of permissions then select the **Directory.AccessAsUser.All** entry.
14. Select **Add Permissions** at the bottom of the page.  
You are returned to the **Configured permissions** pane where **Directory.AccessAsUser.All** has been added to the list of configured permissions.
15. Select **Application permissions**.
16. Locate and open the **Directory** entry in the list of permissions then select the **Directory.Read.All** entry.
17. Select **Add Permissions** at the bottom of the page.  
You are returned to the **Configured permissions** pane where **Directory.Read.All** has been added to the list of configured permissions all. The **Configured permissions** list should now be complete with all three permissions:

- Directory.AccessAsUser.All
- Directory.Read.All
- User.Read

18. Select **Overview** at the top of the left rail and select **Endpoints** at the top of the page.
19. Copy the **Federation Metadata Document** URL. Paste the URL into another browser window to download the metadata. Save the XML as "federationmetadata.xml".
20. Open the hamburger menu in the top left of the screen and select **Azure Active Directory**.
21. On the **Overview** screen that opens, select **Enterprise Applications** from the left rail.
22. Select **All Applications** from the **Application Type** drop-down and select **Apply**.
23. Locate and open your new application.
24. Select **Properties** from the **Manage** section in the left rail.
25. Select **Yes** for **User assignment required**.
26. Select **Yes** for **Visible to users**.
27. Select **Save**.



## Configure SAML in PAM

1. Log in to your PAM instance. If you are setting up a cluster, ensure that the cluster is on. Use the first node in the primary site.
2. Navigate to **Configuration, Security, SAML, RP Configuration**.
3. Complete the following fields:
  - **Entity ID:** Your App ID URL, for example: `https://ip_address`
  - **Friendly Name:** CAPAM
  - **Fully Qualified Hostname:** Your PAM IP address  
For a cluster, each member uses its own IP address.
  - **Certificate Key Pair:** select `gkcert.crt` from the drop-down list.
  - **SAML IdP Metadata Refresh Mode** (optional): To specify a schedule for refreshing Azure federation metadata, specify **Hourly** or **Daily**. (The document from which to read Azure federation metadata must be specified in the **Metadata Refresh Source URL** field on the **Configured Remote SAML IdP** tab.)
4. Select **Save Configuration**.
5. If you are using a cluster, repeat this procedure for each instance, but only entering the IP address in the **Fully Qualified Hostname** field.
6. Select **Configure Remote SAML IdP**.
7. Select **Upload an Identity Provider Metadata**. Select **Choose File** to find "federationmetadata.xml" and **Upload** it.
8. Select the new remote SAML IdP entry on the Configured Remote SAML IdP page, and select **Update**.
9. Edit the **Friendly Name** field to be friendlier, to "Azure IdP," for example.
10. Select the **Allow Just In Time Provisioning** checkbox.
11. Optionally, specify the URL of an Azure federation metadata document from which to periodically refresh Identity Provider data in the **Metadata Refresh Source URL** field. (Only used if the **SAML IdP Metadata Refresh Mode** option on the **RP Configuration** tab is set to Hourly or Daily).
12. Select **OK** to save.
13. Select the **Download Metadata** button. "XsuiteMetadataFor\_*Friendly\_Name*.xml" is saved to your Downloads folder.
14. Open the metadata file and copy each Location field URL. For clusters, there are multiple Locations. For example, in this line, copy the entire URL between the quotes:  
**IPv4**  
 Location="https://12.34.56.78/samlsp/module.php/saml/sp/saml2-acs.php/xsuite-default-sp"  
**IPv6**  
 Location="https://https://https:[fd6d:8d64:af0c:1:0:242:22:233]/samlsp/module.php/saml/sp/saml2-acs.php/xsuite-default-sp"

## Configure SAML in Azure

Now we configure the SAML IdP settings in Azure using the information from Privileged Access Manager.

1. Navigate to **Azure Active Directory, App Registrations**. Open your Azure IdP Application.
2. Select **Authentication** from the **Manage** section in the left rail.
3. In the **Web** section of the **Authentication** screen that opens, remove the existing default **Redirect URI**.
4. Use the **Add URI** control to enter each location that you copied from the PAM metadata file.
5. Select **Save**.
6. Select **Manifest** from the **Manage** section in the left rail.
7. Line 8 on the **Edit Manifest** window shows this text: `"app roles": [],`
8. Enter the following text between the square brackets:

```
{
  "allowedMemberTypes": [
    "User"
```



```

    ],
    "displayName": "Global Administrator",
    "id": "b1d7feb5-d688-4187-b257-42df5b621bfd",
    "isEnabled": true,
    "description": "Allows access to and configuration of all PAM functionality",
    "value": "GlobalAdministrator"
  },
  {
    "allowedMemberTypes": [
      "User"
    ],
    "displayName": "Standard User",
    "id": "86456979-e617-41e3-be5f-243ec00d6113",
    "isEnabled": true,
    "description": "Allows users to access and manage remote devices",
    "value": "StandardUser"
  }
}

```

9. Select **Save**.

10. Navigate to **Azure Active Directory, Enterprise Applications**. On the **All Applications** page that opens, select your Azure IdP Application from the list that is displayed.

11. Select **Assign User and Groups**.

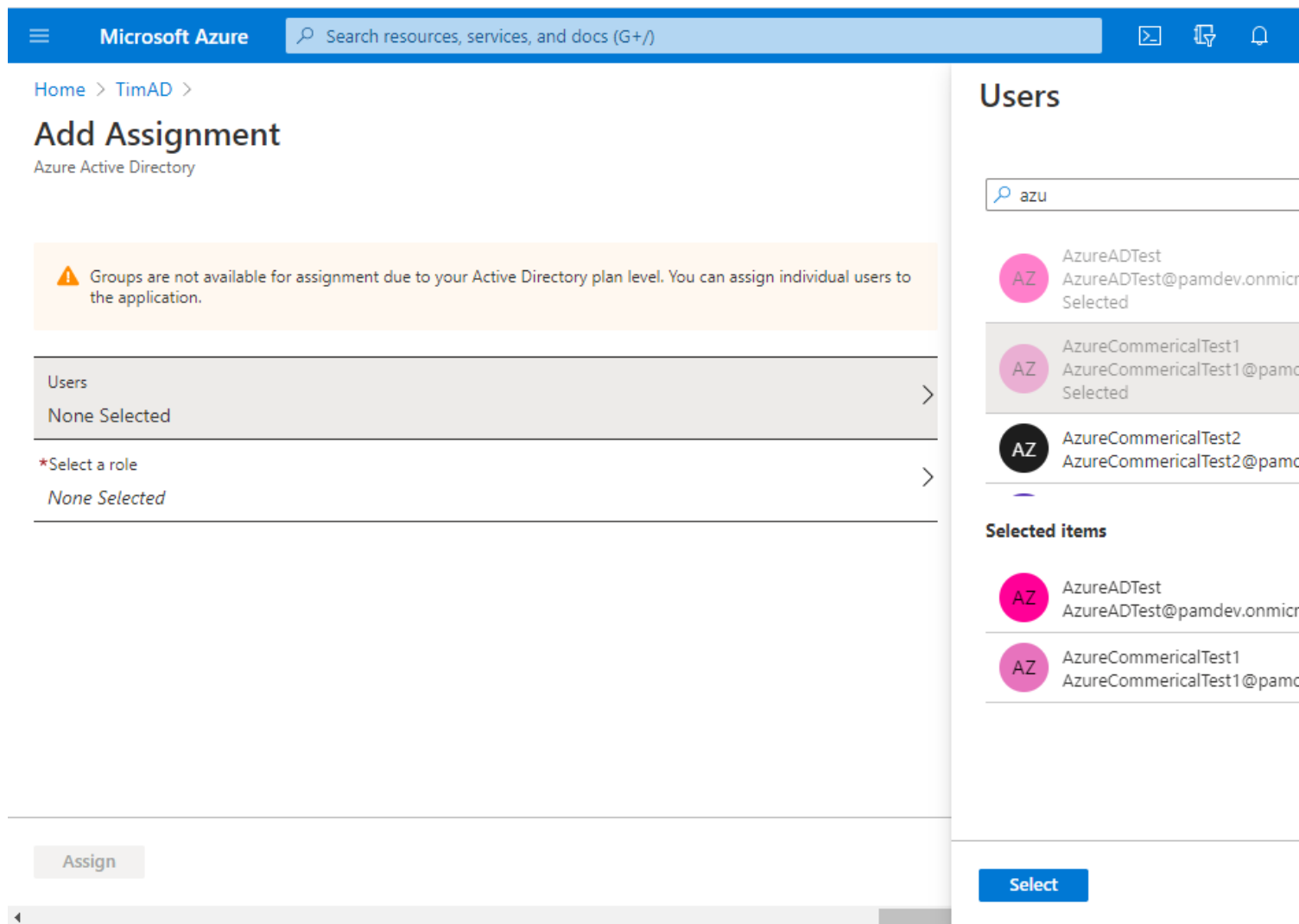
12. Select **+ Add User**.

13. On the **Add Assignment** page that opens, select the **Users** entry, then **select** a user or users from the **Users** list that appears and click **Select**.

**Figure 20: Screenshot showing user selection**

The screenshot shows the Microsoft Azure portal interface. The main heading is "Add Assignment" under "Azure Active Directory". A warning message states: "Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application." Below this, the "Users" section shows "2 users selected." and a role selection dropdown set to "Standard User". The "Assign" button is visible at the bottom left. On the right, the "Users" panel lists three users: "Avishek Sarkar" (as665283@pamdev.onmicrosoft.com), "AzureADTest" (AzureADTest@pamdev.onmicrosoft.com, Selected), and "AzureCommericalTest1" (AzureCommericalTest1@pamdev.onmicrosoft.com, Selected). The "Selected items" section lists "AzureADTest" and "AzureCommericalTest1". A "Select" button is at the bottom right of the Users panel.

14. Select **Select a Role** for the selected user or users, then select a role or roles and click **Select**.

**Figure 21: Screenshot showing role assignment for selected users**

15. Select **Assign**.

### **Create Azure SAML User Group in PAM**

1. In Privileged Access Manager, go to **Users, Manage User Groups**, and select **Add**.
2. Enter the **Group Name** as `AzureSAMLUsers` exactly.
3. Select **OK** to save the group.

### **Create an Azure Target Account and Connection in PAM**

If you have not already configured an Azure Target Account and an Azure Connection, follow the instructions at [Configure an Azure Connection](#).

The Target Account and Connection for Azure in Privileged Access Manager enable these processes:

- Remove active sessions at the next user refresh. This process enhances security because a user could have an active session after their access is revoked.
- Remove and clean up the User in Privileged Access Manager. This process prevents orphaned Azure accounts in Privileged Access Manager.

### **Use Single Sign-On to log in to PAM**

1. Log out from Privileged Access Manager.
2. The login page now has a Single Sign-On link below the Login button.
3. Select the Single Sign-On link.
4. You log in with your Azure AD credentials.

## **Hardware Security Modules (HSMs) for Credential Manager**

By default, Credential Manager uses a software encryption module that is validated to FIPS 140-2 Level 1 (CMVP certificate #3389) to encrypt and decrypt stored credentials. Additionally, a Java encryption module that is validated to FIPS 140-2 (CMVP certificate #3514) is also [implemented](#).

To provide hardware-based encryption to encrypt and decrypt stored credentials, configure one of the following Hardware Security Modules.

- [SafeNet HSM](#)
- [Entrust nShield Connect HSM Appliance](#)
- [Common HSM Features](#)

### **Configure PAM to use a Safenet HSM**

Learn how to configure PAM to use a SafeNet HSM to encrypt and decrypt its stored credentials in place of its built-in cryptographic engine

Configure PAM to use a SafeNet HSM to encrypt and decrypt its stored credentials in place of its built-in cryptographic engine

#### **Configure the SafeNet HSM**

Refer to the Safenet documentation to learn how to configure the Safenet HSM .

#### **Configure Privileged Access Manager**

Although not required, it is recommended that you configure Safenet appliances in Privileged Access Manager only during Privileged Access Manager downtime. If your Privileged Access Manager is a production appliance, plan a maintenance window.

#### **NOTE**

When tested for Privileged Access Manager 2.3, 5000 target account records took approximately 10 minutes to process.

Once Safenet HSM can receive communication, you can configure Privileged Access Manager to use up to three Safenet appliances of the same release level.

#### **Back Up the Database**

Before configuring Privileged Access Manager to engage with the Safenet appliance, back up the Privileged Access Manager database.

**Follow these steps:**

1. Log in to Privileged Access Manager as an administrator (for example, as "super").
2. Navigate to **Configuration, Database**.
3. On the **Database** tab, select **Save Database and Configuration**.  
The page updates with a confirmation of the backup creation with the database (and configuration) filenames. Note the database filename, which should be similar to: gkdatabase20130714124622.gz
4. Click the database filename to select it, and click **Download**.  
The database is saved to your local workstation (or other location).
5. Use this file if you must recover your Privileged Access Manager database.

**Configure the HSM**

The following procedure assumes configuration to one Safenet appliance, and Safenet HSM licensing for Privileged Access Manager. See the section on "Scaling" later in this content for information about changing the number of HSM or Privileged Access Manager appliances.

**Follow these steps:**

1. Log in to Privileged Access Manager as an administrator (for example, as "super").
2. Navigate to **Configuration, 3rd Party, Safenet HSM**.
3. On the **Safenet HSM Configuration** tab, enter the Safenet credentials that you established when setting up the device.
  - a. Enter the **Security Principal Username** you set when configuring the Safenet administrative account.
  - b. Enter the **Security Principal Password** you set when configuring the Safenet administrative account.
  - c. Enter the **Partition Name** as specified during Safenet (5.2 or later) configuration.
  - d. Enter the **Partition Password** you set in the "Create Storage" step during your Safenet configuration procedure earlier.
  - e. Enter the **Address** (IP address or FQDN) assigned to the Safenet appliance.
4. Click **Add** to initiate the configuration.  
After successful account access to the Safenet appliance, the page refreshes, returning with a confirmation message. The **Network Attached HSMs** tab updates with the address (labeled **HSM**), **Status**(showing as *PartitionName: ConnectionStatus*), and permitted **Action** (**Remove** button is available).
5. Reboot Privileged Access Manager.
6. Log back in to Privileged Access Manager, and navigate to the **3rd Party** page.

**NOTE**

Reencryption occurs immediately following a password request from an A2A Client, if that occurs earlier.

Once Safenet Safenet is active, this status is displayed on the [View System Information](#) page.

**Scaling**

Although not required, we recommend that you configure Safenet appliances in Privileged Access Manager only during Privileged Access Manager downtime. If your Privileged Access Manager is a production appliance, plan a maintenance window.

**NOTE**

When tested for Privileged Access Manager 2.3, 5000 target account records took approximately 10 minutes to process.

**Add a Safenet Appliance**

You can add a second and a third Safenet appliance to the Privileged Access Manager configuration. When doing so, repeat the procedures in "Configure Safenet" and "ConfigurePrivileged Access Manager."

**Requirement:** Use the same password for the storage element that you assigned in the **Create Storage** procedure for each Safenet appliance.

### ***Remove a Safenet Appliance***

You can remove a Safenet appliance from an existing Privileged Access Manager configuration.

#### **Follow these steps:**

1. Log in to Privileged Access Manager as an administrator (for example, as "super").
2. Navigate to **Configuration, 3rd Party, Safenet HSM**.
3. On the **Network Attached HSM** tab, click the remove button of a Safenet appliance you want to remove.  
The page refreshes to show removal of the selected appliance.
4. If you have removed the only (remaining) appliance, reboot Privileged Access Manager.
5. Log back in to Privileged Access Manager, and navigate to the **3rd Party** page.

#### **NOTE**

Reencryption occurs immediately following a password request from an A2A Client, if that occurs earlier.

6. Privileged Access Manager does not remove the authorized client from Safenet. Issue the following command on the Safenet HSM:

```
[Safenet] Safenetsh:> client delete -c <hostname> -f
```

Otherwise, if the authorized client is registered on the HSM, and you want to add to HSM again later, you receive an error message: This client is already registered on the HSM.

### ***Share a Safenet (Group) Among Multiple Appliances***

A Safenet HSM appliance or appliance group that has been configured on one Privileged Access Manager appliance may then be configured on more appliances. Follow the procedure in "Privileged Access Manager Configuration" earlier in this content.

**Requirements:** Each Privileged Access Manager appliance must use the same encryption/decryption key.

### ***Share a Safenet Group Within a Cluster***

A Safenet appliance group may be configured for use in an existing Privileged Access Manager synchronized cluster by configuring the devices in the following sequence.

#### **WARNING**

Each member of a Privileged Access Manager cluster must use the same HSM installations – that is, an identical set of **Address** and **Partition Name** combinations should be configured on each Privileged Access Manager.

Assumptions:

- An existing Privileged Access Manager cluster:
  - Primary Privileged Access Manager member (Call this device X1)
  - First Secondary Privileged Access Manager member (X2)
  - Second Secondary Privileged Access Manager member (X3)
- Three Safenet HSM appliances (of the same release level):
  - First HSM (H1)
  - Second HSM (H2)
  - Third HSM (H3)

#### **Follow these steps:**

1. If the Privileged Access Manager cluster is active, stop it. Per the following steps, do **not** restart the cluster again until after all HSMs have been configured on each Privileged Access Manager device.
2. Navigate to **Configuration, 3rd Party, Safenet HSM**.

3. On the **Safenet HSM Configuration** tab on X1, fill in and Add H1.
  - Do **not** reboot (until after all HSMs – H1, H2, and H3 – have been configured on X1).
  - The encryption key must be generated *one time only* on H1, and then must be copied to H2 and H3.
4. After Privileged Access Manager X1 has successfully connected to H1, fill in and Add H2. Do not reboot.
5. After Privileged Access Manager X1 has successfully connected to H2, fill in and Add H3. Do not reboot.
6. Now, reboot (primary cluster member) X1.
7. For (secondary cluster member) X2, repeat steps 2 through 5.
8. For (secondary cluster member) X3, repeat steps 2 through 5.
9. Restart the Privileged Access Manager cluster.

## Configure PAM to use an Entrust nShield Connect or Connect XC HSM

This content describes how to configure PAM to use an Entrust nShield Connect or nShield Connect XC HSM to encrypt and decrypt stored credentials in place of its built-in cryptographic engine

### Prerequisites

Configuring Privileged Access Manager to work with the Entrust HSM requires one of the following the following appliances:

- nShield Connect
- nShield Connect XC hardware appliance

### Deployment Guidelines

Privileged Access Manager can operate with Entrust nShield HSMs according to the following guidelines:

- Entrust nShield Connect 1500 running client software Security World Software version 11.62.00. This client can be used with nShield Connect versions: 500, 6000, and 6000+
- Entrust nShield Connect XC running client software Security World Software, version 12.40.2. This client can be used with the following nShield Connect XC versions: XC Base, XC Mid, and XC High

### Configure Entrust nShield Connect or nShield Connect XC

Before you can configure communication with the nShield HSM, prepare the HSM to recognize Privileged Access Manager.

#### **NOTE**

The following procedures describe a third-party environment (Entrust nShield Connect 7.1) that is outside Broadcom control. The procedures are representative examples of the interface. For installation instructions, see the manufacturer documentation for your nShield product.

For Entrust Security World Software 11.62.00, refer to these following documents that come with the Entrust product:

- nShield\_Connect\_Quick\_Start\_Guide.pdf, referred to as INSTALL GUIDE in the following procedure
- nShield\_Connect\_and\_nethSM\_User\_Guide.pdf, referred to as the USER GUIDE in the following procedure

For Entrust Security World Software 12.40.2, refer to these following documents that come with the Entrust product:

- nShield\_Connect\_Installation\_Guide.pdf, referred to as the INSTALL GUIDE in the following procedure
- nShield\_Connect\_User\_Guide\_Unix.pdf, referred to as the USER GUIDE in the following procedure
- nShield\_Connect\_User\_Guide\_Windows.pdf, referred to as the USER GUIDE in the following procedure

**Follow these steps:**

1. Install and configure the nShield appliance. You must follow the INSTALL GUIDE to install and configure the HSM on the network.
2. Note the nShield appliance Ethernet interface IP address. This address is entered in later when setting up PAM. You *cannot* use an FQDN or other DNS name.
3. Create a Security World: You must create a security world as described in Chapter 7 of the USER GUIDE.
4. Create an Operator Card Set.  
An Operator Card Set (OCS) contains one or more smart cards that are used by the nShield Security World. These cards protect all cryptographic secrets that PAM can create. You must create an Operator card Set as described in Chapter 8 of the USER GUIDE document.
5. Make note of the **OCS name** and **passphrase**. The PAM setup uses these values.  
This OCS must be a "1 of N" set, where N is at least the number of HSMs. N can be greater than that number, but the OCS must be 1 of N.

**WARNING**

When creating an operator card set with more than one card, each card must have the same OCS name and password. Both the name and password are user selectable.

Using the same name and password allow PAM to use multiple nShield HSMs as a failover group. Also, PAM searches the nShield device for the operator card based on its name, so the name on each card in a set must be the same.

The standard OCS is non-persistent, means you can only use the keys protected by that OCS while the required card remains loaded in the smart card reader of the nShield device. The keys protected by this card are removed from the memory of the hardware security device as soon as the card is removed from the smart card reader. Although this feature provides added security, it means that only a single user can load keys at any given time.

**NOTE**

If the required card cannot remain loaded in the smart card reader, you must create a **persistent** Operator card set. This is described in Chapter 8, in the "Persistent Operator Card Sets" section of the USER GUIDE document.

6. Create the Remote File System (RFS): You must create a "Remote File System" as described in Chapter 6 of the USER GUIDE document. The RFS stores configuration data and shared secrets for clustered clients (PAM instances) that share a single HSM or a group of HSMs.  
Note of the client computer IP address on which you set up the RFS. This address is entered when you set up PAM. Do *not* enter an FQDN.
7. Register the PAM IP address on the nShield.  
You must register the PAM IP address as a client onto the nShield device. **This is done on the front panel of the nShield device**, and is described in Chapter 6, in the "Configuring the unit to use the client" or "Configuring the nShield Connect to use the client" section of the USER GUIDE document.  
During the process, configure PAM as a "**non-privileged**" client and does **NOT** use an nToken device.  
To add PAM IP address as a client remotely on the Remote File System (avoid the need to access the nShield device), see the "Remote configuration of additional clients" section in Chapter 6 of the USER GUIDE document.
8. PAM IP address registration on the RFS.  
You must register the PAM IP address on the Remote File System to allow for PAM clustering where multiple PAM in a cluster could share an nShield device. **This is done on the computer that acts as the RFS** and is described in the section entitled "Setting up client cooperation" in Chapter 6 of the USER GUIDE document.

**TIP**

For PAM clustering (multiple PAM instances) to work, it must have 'gang-client' argument in the rfs-setup command.

Depending on your environment, you can use either Method 1 or Method 2:

**Method 1:**



For every unauthenticated client (with write access but without **KNETI** authorization) that needs to be a client of this remote file system, run the command on the RFS machine:

```
rfs-setup --gang-client --write-noauth PAM_IP_address
```

#### NOTE

The **--write-noauth** option should only be used if you believe your network is secure. This option allows the client you are configuring to access the RFS without KNETI authorization.

#### Method 2:

For every authenticated client (with write access and KNETI authorization) that needs to be a client of this remote file system, run the command on the RFS machine:

```
rfs-setup --gang-client PAM_IP_address EEEE-SSSS-NNNN keyhash
```

- **EEEE-SSSS-NNNN** is the ESN of the unit
- **keyhash** is the hash of the KNETI key on the unit.

#### TIP

To retrieve the unit's **ESN** and **KNETI**, run the following command:

```
anonkneti nShield_device_IP_address
```

### Configure PAM to Use the HSM

After a Entrust nShield Connect HSM is set up, configure PAM. The configuration enables PAM to establish communication with up to three nShield HSMs of the same release.

To identify the Entrust HSM to PAM, complete the following steps:

1. Install the license.
2. Back up the database.
3. Identify the HSM to PAM

#### WARNING

We recommended that you configure PAM to use nShield HSMs only during downtime. For a PAM appliance in production, plan a maintenance window.

#### Install the License

Before you configure communication with the HSMs, install the Privileged Access Manager license for HSM use.

#### Back Up the Database

Adding an HSM configuration triggers reencryption of all passwords in the database. Before configuring Privileged Access Manager to engage with the nShield appliance, back up the database.

1. Log in to the UI as an administrator (for example, as "super").
2. Navigate to **Configuration, Database**.
3. On the **Database** tab, click **Save Database and Configuration**.  
The page updates and displays the backup file names. Note the database filename, such as gkdatabase20130714124622.gz
4. Select the database filename from the file list, and click **Download**.  
The database is saved to your local workstation (or other location).

Use this backup file to recover your database if necessary.

#### Configure the HSM Settings in

**WARNING**

Before you reboot PAM or restart a cluster, verify that the OCS smart card is inserted into the Entrust nShield HSM. After PAM is successfully communicating with the HSM, you can remove the card. If PAM loses network connectivity to the HSM, the card might also be required to re-establish the connection.

The following procedure assumes configuration to one nShield HSM appliance.

1. Log in to the UI as an administrator (for example, as "super").
2. Navigate to **Configuration, 3rd Party, Entrust HSM**.
3. On the **Entrust HSM Configuration** tab, enter the nShield credentials that are used to configure the nShield HSM.
  - a. In the **Token Label** field, enter the name of the OCS.
  - b. Enter the IP address (not a DNS name) of the client computer on which you set up the Remote File System.

**NOTE**

The default port for the two nShield address parameters is 9004. If you are not using the default port, specify the alternate port number in a full socket declaration. For example: 192.168.0.2:9999

- c. In the **Token Password** field, enter the password of the OCS.
  - d. In the **Address** field, enter the IP address (not a DNS name) assigned to the nShield appliance.
4. Click **Add** to initiate the configuration.
  - If you are configuring a *first* HSM, all passwords in the database are reencrypted. A dialog appears, warning you of this effect and allowing you to cancel.
  - If you are configuring a second or third HSM, no reencryption or dialog occurs.

During the process of changing from native Privileged Access Manager to nShield encryption, the Credential Manager database is copied to the nShield appliance. While the database is copied, the existing Credential Manager database is still available for use for other purposes.

After successful account access to the nShield appliance, the page refreshes with a confirmation message. An updated Networked Attached HSMs tab appears with the address and status of the appliance.

5. Reboot Privileged Access Manager.
6. Log back in to Privileged Access Manager and navigate back to the **3rd Party** page.
7. Confirm the required reencryption of passwords.

This reencryption also occurs immediately following a password request from an A2A Client, if that occurs earlier.

Once Entrust nShield is active, this status is displayed on the [View System Information](#) page.

**Add or Remove HSMs**

You can change the Privileged Access Manager configuration of HSMs to add or remove one or more HSMs, or update the stored OCS password.

We strongly recommend that you configure nShield appliances in Privileged Access Manager only during downtime. If your Privileged Access Manager is a production appliance, plan a maintenance window.

**WARNING**

Before you reboot PAM or restart a cluster, verify that the OCS smart card is inserted into the Entrust nShield HSM. After PAM is successfully communicating with the HSM, you can remove the card. If PAM loses network connectivity to the HSM, the card might also be required to re-establish the connection.

**Add HSMs**

You can add one or two more HSMs for Privileged Access Manager. A maximum of three HSMs is allowed.

**Follow these steps:**

1. Log in to the UI as an administrator (for example, as "super").
2. Navigate to **Configuration, 3rd Party**, and expand it.

3. On the **Entrust HSM Configuration** tab, enter the nShield credentials that are used to configure the nShield HSM.
  - a. In the **Token Label** field, enter the name of the OCS.
  - b. Enter the IP address (not a DNS name) of the client computer on which you set up the Remote File System.

#### NOTE

The default port for the two nShield address parameters is 9004. If you are not using the default port, specify the alternate port number in a full socket declaration. For example: 192.168.0.2:9999

- c. In the **Token Password** field, enter the password of the OCS.
  - d. In the **Address** field, enter the IP address (not a DNS name) assigned to the nShield appliance.
4. Click **Add** to initiate the configuration.  
After successful account access to the nShield appliance, the page refreshes with a confirmation message. The **Network Attached HSMs** tab is updated.
5. Reboot Privileged Access Manager.
6. Log back in to Privileged Access Manager, and navigate to the **3rd Party** page.
7. Initiate the required re-encryption of passwords.

This re-encryption also occurs immediately following a password request from an A2A Client, if that occurs earlier.

The Token Password value must be the same one that you used for the first HSM. Otherwise, you must reconfigure your other HSM OCS.

#### ***Remove HSMs to Revert Encryption***

To revert the encryption mechanism back to Credential Manager, remove HSMs.

#### **Follow these steps:**

1. Log in to the UI as an administrator (for example, as "super").
2. Navigate to **Configuration, 3rd Party**.  
The **Networked Attached HSMs** tab shows one or more HSMs.
3. Confirm that the HSM or HSMs are online.
4. Next to the HSM you want to remove, click **Remove**.  
If only one HSM is configured, a message indicates that the removal triggers re-encryption of all passwords in the database. The passwords are reassigned to Credential Manager. Following the re-encryption process, you see a Success or an Error message.
5. Reboot Privileged Access Manager.
6. Log back in to the UI, and navigate back to the **3rd Party** page.  
The HSM is no longer being used.
7. Confirm the required re-encryption of passwords.  
This reencryption also occurs immediately following a password request from an A2A Client, if that occurs earlier.

#### **Configure a Cluster to Work with an nShield Group**

An nShield HSM or HSM group can be configured for use in an existing Privileged Access Manager synchronized cluster.

The following procedure assumes the following setup:

- An existing *n*-member cluster is configured.
- Up to three nShield HSM appliances (of the same release level) are installed in the network.

#### **Follow these steps:**

1. On the primary PAMcluster member:
  - a. Complete all preliminary procedures (license installation, database backup), if needed.
  - b. For every HSM in the network, [Configure the HSM Settings in PAM](#).
2. For each additional cluster member, [Configure the HSM Settings in PAM](#).

All members of the cluster can now use the Entrust HSM.

## Common HSM Features

The following features apply to all brands of HSMs.

### Updating Passwords

You can update the Token Password of an installed Entrust nShield HSM, or the Partition Password of an installed SafeNet Luna SA HSM, without taking the HSM offline.

1. On the HSM appliance or appliances, change the relevant HSM password. (See the manufacturer documentation.)
2. In Privileged Access Manager web UI or Client, navigate to **Configuration, 3rd Party**, and your HSM module (Entrust or SafeNet).
3. On the **Network Attached HSMs** tab, confirm that the HSM Status field shows "online."  
For example, for an Entrust HSM:  
In the Entrust HSM Configuration staging panel, enter the new password in the second Token Password field at the bottom of the panel. This field is next to the Update and Activate button.

#### NOTE

Because the password field characters are hidden, you can copy and paste the password instead of typing the password to avoid data entry errors. If you have multiple HSMs, the Token Password is the same on each, so you do not have to identify the specific appliance.

4. Click **Update & Activate**.

A response is presented at the top of the **3rd Party** page:

- If the password is correct, you the following response appears:  
"Success updating the HSM password."
- If the password is *not* correct, or if there was a problem communicating with the HSM, the following response appears:  
"Error the HSM password is incorrect."

## AWS Coordination

As a Privileged Access Manager Administrator, you can configure access to one or more regions in one or more Amazon Web Services accounts. You can then import AWS instances as Privileged Access Manager Devices and provide controlled, account-obfuscated end-user access to the AWS Management Console. Credentials for a particular AWS account are stored as an individual target account in Credential Manager. Using an enhanced configuration interface, you can provision combinations of AWS accounts and regions for concurrent connection.

Configuration allows these types of coordination:

- Configuration of restricted access to the AWS Management Console website for any policy-enabled Privileged Access Manager user
- Import, and regular refresh, of all active AWS devices (in the configured AWS region) as Privileged Access Manager devices

Follow these procedures:

1. [Obtain an AWS account](#) with at least the following privileges:
  - ec2:DescribeInstances
  - ec2:DescribeTags
2. [Store AWS Account Credentials in a Privileged Access Manager CM.](#)
3. (Optional) [Configure AWS Connection](#)
4. (Optional) [Configure AWS Settings](#)

5. (Optional) [Provision AWS Management Console Access](#)
6. (Optional) [Apply AWS Policy Settings](#)
7. (Optional) [More Account/Region Specific Configuration](#)
8. (Optional) [Clustering](#)

#### NOTE

To use Privileged Access Manager with AWS, you apply a license with AWS Capability Enabled. You can verify the license on the **Configuration, Licensing** page.

### **Obtain an AWS Account**

You identify an accessible AWS account before configuring Privileged Access Manager to communicate with it. Your organization might already have such an account, or you can set one up at <https://aws.amazon.com>.

#### NOTE

The AWS account must have at least the following privileges:

- ec2:DescribeInstances
- ec2:DescribeTags

Note the character strings for these AWS objects:

- Access Key ID
- Secret Access Key

Select and note the following AWS view:

- AWS (geographical) region - for example, **US East (N. Virginia)**

### **Store AWS Account Credentials in Privileged Access Manager**

So that Privileged Access Manager can coordinate with AWS, first store your AWS account credentials in a target account record in Privileged Access Manager Credential Manager.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. The Target Accounts page opens.
2. Select **Add**.
3. Begin typing AWS in the **Application Name** field, and select **AWS Access Credential Accounts** from the drop-down list. Alternatively, select the magnifying glass icon to open a modal window to select this application. The **Host Name** and **Device Name** are populated with the AWS-specific names.
4. In the **Access Key** field, assign a user-friendly unique label for your AWS account.
5. Fill in the **Access Key ID** and **Secret Access Key** you collected from AWS.
6. (Optional) If applicable, assign an **Access Role Name**.
7. (Optional) If you use AWS GovCloud, in **AWS Cloud Type** select **Government**.
8. Do not populate any other fields or change any other settings.
9. Select **OK**.

Privileged Access Manager can now use your AWS access credentials for auto-connection in multiple scenarios.

### **Configure AWS Connection**

After you have stored your account credentials, you point to them in your Privileged Access Manager-to-AWS configuration settings and activate a connection.

**Follow these steps:**

1. Select **Configuration, 3rd Party, AWS**.  
The Amazon Web Services (AWS) panel appears.
2. Select the **Add** button.  
The **Add AWS Connection** window appears.
3. Select your previously set user-friendly Account Name from the **Access Key** drop-down list.
4. In the **Region** field, select your applicable geographical region.
5. (Optional) Select the **Active** checkbox to prompt importing devices with (AWS) State="running" (without an AWS "Xsuitelgnore" tag). Otherwise, only the validity of your stored account-region pair is tested.

**NOTE**

For clustered environments, to avoid importing devices multiple times, causing duplicate device conflicts and exceeding your license, only set the primary member of the primary site as "Active."

6. Select **OK** to confirm the connection, and if activated, perform the initial account-region device import from AWS. You receive a confirmation at the top of the page that the connection has been validated. The **AWS Configured Configurations** tab displays an account-region line item.

Your Privileged Access Manager connection to this AWS account is now activated for the selected region. The connection is available for access to AWS Management Console and is used for importing devices. The imported devices are visible and available for use on the **Devices, Manage Devices** page, where you can edit the Privileged Access Manager-applied (not the imported) fields.

**Configure AWS Settings**

Use these steps to set the refresh rate as well as the how to display the **Access Key** field in the UI.

**NOTE**

Upon upgrade to version 3.4.4 or later, the **Use ID** becomes the default: this setting makes the **Access Key ID** the default display name.

**Follow these steps:**

1. Select **Configuration, 3rd Party, AWS**.  
The Amazon Web Services (AWS) panel appears.
2. Select the **AWS Settings**. See the following Configure AWS Settings:
  - a. In the **Refresh Interval** field, enter the frequency of the download of device information from Amazon. Interval defaults to 60 minutes, but can also be set to 15, 30, or 45 minutes. You can also
  - b. Select how to display the **Access Key** field in the UI:
    - Select the **Use Alias** radio button to display the more user-friendly value, Access Key Alias, in the UI.
    - Select the **Use ID** radio button to display the AWS-generated Access Key ID in the UI.
3. Select **OK**.

**NOTE**

All other currently-open pages that have the AWS credentials loaded must be refreshed for this change to take place.

**Provision AWS Management Console Access**

After you store your account credentials, set a user policy with a controlled-access web portal that opens the AWS Management Console.

**Follow these steps:**

1. Select **Policies, Manage Policies**.

The Manage Policies page opens.

2. Select the **Add** button.

The Add Policy window appears.

3. In the **User** or **User Group** field, start typing the User or User Group you want the policy to apply to. Select the matching full name from a filtered drop-down list.
4. In the **Device** field, select **http://xceedium.aws.amazon.com** from the drop-down filtered list.
5. Set up the policy link:
  - a. Select the **Services** tab, and select **AWS Management Console SSO**. Select the arrow to move the service to Selected Services.
  - b. In the Target Account files next to the service, select **AWS Access Credential Accounts - Access Key**.
  - c. Select in the field marked **AWS Policy**, and select an available setting, such as **IAMUserAccess**.
6. Select **OK**.  
On their **Access** page, provisioned users and user group members should now have a web portal type link **AWS Management Console SSO** for device **http://xceedium.aws.amazon.com**.
7. Log into PAM using an AWS-provisioned user or user group member and select the **AWS Management Console SSO** link.
8. On the **Available Credentials** dialog that appears, select the **userID-govcloud** entry. If you cannot access the AWS GovCloud, ask the AWS GovCloud administrator to assign, at minimum, the following policy to the **userID-govcloud** account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:GetFederationToken",
      "Resource": [
        "arn:aws-us-gov:sts::*:federated-user/*"
      ]
    }
  ]
}
```

For more information about AWS policies and permissions, see [https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html).

### **Apply AWS Policy Settings**

To ensure transparent login access to this site from Privileged Access Manager, the AWS Management Console requires a current, appropriate AWS policy. The default settings and any custom settings require communication with AWS. See [http://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_inline-using.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_inline-using.html) for more information.

#### **Follow these steps:**

1. In **Policies, Manage Policies**, Select the **AWS Policies** link.
2. Select an existing, or create a new, AWS Policy.
3. Apply the following AWS IAM policy settings to its **Policy** field, and Select **OK**:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:GetFederationToken",
```



```

        "Resource": "*"
    }
}
]
}

```

4. Be sure to use this revised AWS Policy in the Services policy template for an applicable User with "http://xceedium.aws.amazon.com".

### **More Account/Region Specific Configuration**

#### ***S3 Mounts***

Amazon S3 mounts can no longer be assumed in the (sole) AWS Account and Region that are specified in release 2.2.0. On the **Configuration, Logs, Session Recording** page, **NFS/CIFS/S3 Settings**, you must explicitly identify which **AWS Provision** (Account and Region) to use.

#### **WARNING**

**Warning:** If there is an active S3 mount using a particular **Configuration, Logs, Session Recording, NFS/CIFS/S3 Settings, Amazon S3** provision setting at the time you attempt to remove its corresponding connection from **Configuration, 3rd Party, Amazon Web Services (AWS) Configuration**, the connection is not dropped. The mount remains intact, and an error message is displayed on the **3rd Party** page.

#### **Clustering**

The members of a Privileged Access Manager synchronization cluster that is created within AWS must be located within the same AWS VPC subnet.

Synchronization can no longer be assumed in the (sole) AWS Account and Region that are specified in release 2.2.0. On the **Configuration, 3rd Party, Clustering** page, you must explicitly identify which **AWS Provision** (Account and Region) is being used.

When configuring your AWS connections (see [Configure AWS Connection](#)), set only the primary member of the primary site as "Active." This restriction helps you avoid importing devices multiple times, causing duplicate device conflicts, and exceeding your license.

#### **NOTE**

- [Integrating an AWS API Proxy \(Optional\)](#)

## **Configure and Manage Session Recording**

Configure session recording to enable PAM to create and store recordings of supported (CLI, RDP, VNC, and Web Portal) connection sessions.

### **Session Recording Overview**

Each session recording is stored or referenced within PAM using the following elements:

- The recording itself, in a media file (with associated file extension) corresponding to the nature of the session:
  - **RDP session:** `.gsr` graphical session recording file.
  - **VNC session:** `.vsr` graphical session recording file.
  - **SSH session:** `.txt` CLI (text-based) session recording file.
- A *metadata file* that contains information about the session recording. These metadata files are created by session recording reconciliation, which is described in the following section.



**IMPORTANT**

Metadata files have the *same name* as the session recording with which they are associated but with a **.inf** extension. For example, the metadata file that is associated with `session_recording_filename_1.gsr` is `session_recording_filename_1.inf`

**NOTE**

There are also other session recording file types that are used internally. You can ignore these, but *do not delete* them.

- An entry in the *session recording database* that references the session recording media file and information about the recording from the metadata file. The session recording database is used to populate the **Session Recording Viewer**.

**Session Recording Reconciliation**

PAM runs the following *session recording reconciliation processes* that identify session recordings that do not have a corresponding metadata file or database entry and, if so, creates the missing element:

- **Most Recent Recordings:** Reconciles recent session recordings. Runs hourly.
- **All Other Recordings:** Reconciles other session recordings. Runs daily.
- **Restored Recordings:** Reconciles session recordings [recovered from archives](#). Runs hourly.

**TIP**

You can check the status of the session recording reconciliation processes on the [System Info pane](#) **System Activity** tab.

**NOTE**

Session recording reconciliation processes do not run while a PAM server is in maintenance mode.

**Mount an NFS, CIFS, or S3 Network Share for Session Recordings**

Text-based recordings can be stored on a remote syslog server, a mounted network share, or both. Graphical recordings must be stored on a mounted NFS, CIFS, or S3 network share.

This procedure describes how to mount an NFS, CIFS, or S3 network share to enable recording for graphical or text-based session recordings.

**NOTE**

For information about syslog servers, see [Remote Syslog Server Configuration](#)

**NOTE**

When mounting an NFS or CIFS share for session recordings, configure appropriate privileges for the specified directory on the host system. For an NFS share, grant read, write, and execute permissions (`rwx`) to everybody. For a CIFS share, grant **Full Control** to **Everyone**.

**Follow these steps:**

1. Navigate to **Configuration, Logs, Session Recording**.
2. Select the **External Storage** tab.
3. In the **Primary Mount Settings** section, select one of the following network share protocols from the **Protocol** drop-down list:
  - NFS (version 3 and 4 are supported)
  - CIFS
  - Amazon S3
  - NFS (Verify Certificate)
 Option fields relating to the selected protocol are displayed below the **Protocol** drop-down list.
4. Complete the option fields that are associated with the selected protocol:
  - **NFS:**

- **Share Path:** Enter the directory path name of the NFS mount point.

**IMPORTANT**

In a multi-cluster environment, you must configure a separate NFS mount point for each cluster.

**WARNING**

Do not use the same NFS mount point that you are using for [scheduled database backups](#). The session recording and scheduled database backup processes create and delete a file with the same name to check the remote storage status. If you specify the same NFS mount point, file locking can occur as both processes attempt to create or delete the same file.

- **Hostname:** Enter the IP address or hostname of the server with the share.
- **Request Timeout:** Optionally, enter a non-default timeout value (in tenths of a second) for NFS requests. If no value is specified, the default is determined by the NFS server, typically 600.

**NOTE**

We recommend that if the NFS server does not respond quickly enough that you accept the default **Request Timeout** to avoid latency. However, if NFS storage is down, you can set a lower value to receive early notification.

- **Encrypt in Transit:** Allows PAM to send session recording data over a secure (TLS) channel. No remote server certificate verification is performed. If remote server certificate verification is required, select NFS (Verify Certificate) protocol.

– **CIFS:**

- **Share Path:** Specify the mount point using the format `\\hostname\share` . (You can also use forward slashes.)
- **Username:** Specify a user who has read and write access to the remote share.
- **Password:** Specify the password for that user.
- **Domain:** Specify the CIFS domain.
- **SMB Version:** Select the version of Server Message Block that is used by the target system. Newer versions of SMB are more secure. If you no longer support older file shares (like Windows 2003), we recommend using SMB2 or SMB3, provided the CIFS system supports it.

**NOTE**

Azure does not support mounting an Azure file share in a different region than your Azure Privileged Access Manager VM.

– **Amazon S3:**

- **Bucket:** Enter the AWS bucket to use.
- **AWS Provision:** Select the appropriate entry from the drop-down list.

**NFS (Verify Certificate):**

- **Encrypt in Transit:** Allows PAM to send session recording over a secure (TLS) channel.
- **Verify Certificate Chain:** Allows PAM to verify the remote server certificate and the complete chain of the remote server certificate.
- **Verify Hostname(s):** Specifying one or more hostnames allows PAM to check if the certificate Subject Alternative Name (SAN) or Subject Common Name (CN) matches the specific host names.

**NOTE**

The **Verify Certificate Chain** and **Verify Hostname(s)** options involve verification of a remote server certificate. The CA bundle, including the public key of the remote server certificate, must be uploaded into PAM. Select **Configuration, Security, Certificate, CA Bundles**.

5. Select **Save Settings**.

A confirmation message appears at the top of the screen.

6. Select **Mount**.

A success or an error message appears at the top of the page.

**IMPORTANT**

If you must unmount a configured NFS share and restart the NFS server, wait at least 2 minutes for the NFS share to become available before attempting to remount that share.

**Network Mount Point Subdirectories**

PAM stores session recordings in the following subdirectories that it creates under the configured mount point::

- On each day that sessions are recorded, a correspondingly named *daily subdirectory* (*YYYYMMDDPAM*) to store those recordings. For example, if the mount point share path is `/var/nfsshare`, the session recordings for Jun 7, 2022, are stored in `/var/nfsshare/20220607PAM`.

**NOTE**

The daily subfolders are transparent to session viewers; the physical location of files is not shown on the **View Session Recordings** panel.

- A `recoverPAM` subdirectory that is used when restoring archived files. For example, if the mount point share path is `/var/cifsshare`, the `recoverPAM` subdirectory is located at `/var/cifsshare/recoverPAM`. For more information, see [Archive and Recover Session Recording Files](#).

**Verify the Status of a Mount**

The **Mount Status** field displays whether the share is mounted or unmounted. If the share is mounted, **Mount Status** displays the status of the mount: **available** or **unavailable**

If **Mount Status** shows **unavailable**, the share is still mounted but not currently accessible (for example, due to network problems or share permissions). In this case, there is no need to remount the share. When the issue causing the share to be inaccessible is resolved, the status changes back to **available**

**WARNING**

By default, an access policy can specify that a session is to be recorded. If the configured network share becomes unavailable, users cannot establish a connection to the share. To allow such sessions to connect anyway, change the [session recording access policy](#) to **Connect anyway. (Operationally Safe)** For optimal security, we recommend that you keep the default access policy and configure [session recording failover](#).

**(Optional) Set Up Session Recording Failover**

To avoid losing session recording ability due to a storage failure, mount a secondary share to provide failover. Session recording failover dynamically switches over to the secondary share without any loss of data. While the secondary share is in use, you cannot view session recordings on the secondary or the primary share until the primary is restored. To restore session recording on the primary share, the primary share must be back online. When the primary share comes back online, recordings that were split across the two shares are automatically recombined. You can then view the recordings seamlessly.

To configure failover mount settings, navigate to **Configuration, Logs, Session Recording, External Storage**. The configuration for the failover mount settings is identical to the configuration for [Primary Mount Settings](#).

**Activate Session Recording**

To active session recording, specify one or more of the types of sessions that you want to record.

**Follow these steps:**

- Navigate to **Configuration, Logs, Session Recording**.
- Select the **Session Recording** tab.
- Specify the types of sessions that you want to record. Set one or more of the following options on the **Configuration, Logs, Session Recording** screen:

- **Text-based recording to the syslog server**
- **Text-based recording to a NFS/CIFS/S3 mounted directory**
- **Graphical session recording to a NFS/CIFS/S3 mounted directory**

These recording options are unavailable until you configure the required [syslog server](#) or network mounts.

4. **Allow External Storage for Large Session Recording Decryption:** If storage on your appliance becomes limited, large session recording files might become unviewable. Select this option to allow the decryption of large session recordings on the external storage. We attempt to use appliance storage first, and only use external storage when necessary. The decrypted files are deleted from external storage periodically. If you never want decrypted session recording files on your own storage, leave this option in its default cleared state.
5. Select the **UPDATE** button to save your changes.

#### NOTE

To prevent failures, unset the appropriate option if a share is nearing capacity.

### Specify Which Sessions to Record

Use one of the following mechanisms to record sessions:

- **Automatically, by policy** – When provisioning a policy in each **Policies, Manage Policies**, User/Device record, you can elect to activate recording based on the following criteria:
  - Media type: graphical, command line, bidirectional command line, web portal
  - On violation: socket filter or command filter violation
 For more information, see [Set Up a Policy](#).
- **Manual** – Privileged Access Manager administrators can activate session recording while a session is taking place using controls on the **Sessions, Manage Sessions** screen. Each session line item has a recording stop/start switch. For more information, see [Session Management](#).

#### TIP

View recorded sessions from the **Sessions, Session Recording** panel. For more information, see [View Session Recordings](#).

### Change the Session Recording Access Policy

By default, if the configured network mount becomes unavailable, users cannot establish a connection if their session should be recorded. Use the controls on the **Access Policy** tab to change the access policy to allow such sessions to connect anyway.

#### NOTE

For optimal security, we recommend that you keep the default setting and configure [session recording failover](#), described in this topic.

#### Follow these steps:

1. Navigate to **Configuration, Logs, Session Recording**.
2. Select the **Access Policy** tab.
3. Select one of the following options to dictate how the product responds if the session recording mount is unavailable:
  - **Present an error and do not connect. (Security Safe):** This option is the default. If a User is configured for session recording and the mount point is unavailable, do not allow the User to connect to the target device. The **Error Message** entered in the text box is presented to the User. If the mount point is lost during a previous session, the User connection is terminated.
  - **Connect anyway. (Operationally Safe):** If a user is configured for session recording and the mount point is unavailable, allow the user to connect to the target device anyway. Users are not inhibited from accessing the device, but no session recording is created for this session. If the mount point is lost during a previously started session, the user is allowed to continue, but their session is no longer recorded.

4. (Optional) Specify a non-default **Initial Failure Timeout** value (in seconds). The default value is 300.
5. (Optional) If you set the **Present an error and do not connect** option in Step 3, you can enter an **Error Message**. This error message is displayed if a user cannot connect or has been disconnected because of a mount error. If nothing is entered in this field, a generic message is presented.
6. Select the **UPDATE** button to save your changes.

#### **(Optional) Configure a Session Recording Purge Policy**

Optionally, configure a session recording purge policy to set up automatic deletion of session recordings after a specified number of days.

##### **NOTE**

The purge job runs nightly at midnight UTC.

##### **Follow these steps:**

1. Navigate to **Configuration, Logs, Session Recording**.
2. Select the **Purge Policy** tab.
3. Specify the number of days after which session recordings are automatically purged in the **Remove Records Older Than** field. For example, if you set **Remove records older than** to 5, session recordings made more than five days ago are purged

##### **NOTE**

To disable automatic purging of session recordings, set the **Remove records older than** value to zero (0).

4. Specify the number of days after which restored session recordings are automatically purged in the **Remove Restored Recordings Older Than** field. For example, if you set **Remove Restored Recordings Older Than** to 5, session recordings made more than five days ago are purged
5. To purge recordings that include violations, unset the **Exclude Recordings With Violations** option. When the "exclude" checkbox is selected, you retain recordings with violations rather than purge them.
6. To purge recordings that are identified as suspicious by Symantec Threat Analytics, unset the **Exclude Suspicious Recordings** option. When the "exclude" checkbox is selected, you retain suspicious recordings rather than purge them.
7. Select the **UPDATE** button to save your changes.

#### **(Optional) Archive and Restore Session Recordings**

To preserve sensitive session recording files that you might require later (for example, recordings that show suspicious activity), *archive* them to another location. You can then restore those files for viewing in the PAM UI later (for example, for a security audit).

##### **NOTE**

Archiving sensitive files is important if you have configured a purge policy that would otherwise delete them.

##### **To archive session recording files, do the following steps:**

1. Log in to the physical or virtual host where the session recordings are stored.

##### **NOTE**

Text-based recordings can be stored on a remote syslog server, a mounted network share, or both.  
Graphical recordings can be stored on a mounted NFS, CIFS, or S3 network share.

2. Navigate to the file system location in which the session recordings are stored.

##### **NOTE**

Recordings made by PAM versions earlier than 4.1.1 are stored directly in the mounted directory. Recordings that are made by PAM version 4.1.1 and later are stored in subdirectories that are created and named for the day on which they were recorded (*YYYYMMDDPAM*).

3. Locate the session recording files that you want to archive.
4. Copy or move the recording files *and their associated metadata files* to a designated archive location.

**To restore archived session recording files for viewing, do the following steps:**

1. Locate the session recording files and their associated metadata files in the archive location.
2. Move the files to the `mountpoint_sharepath/recoverPAM` directory. For example, if the mount point share path is `/var/cifsshare`, the `recoverPAM` directory is located at `/var/cifsshare/recoverPAM`.

Within an hour, a session recording reconciliation process restores the files to the session recording table in the database and the recordings appear in the **Session Recording Viewer**.

## Use Logs to Monitor Operations and User Sessions

As an administrator, set up the logs to audit server operation, monitor user sessions and log session recordings.

Two types of server log files are available:

- Session logs, which collect user activity
- Syslog, which captures system operations

You can also specify a Splunk server to collect and log appliance behavior. To specify a Splunk server, go to **Configuration, 3rd Party, Splunk**.

The following topics discuss these two logs:

### Session Logs for User Activity

The session logs contain records that capture user activities. These logs are stored in an internal MySQL database, or you can route them to an external MySQL server. For clustered systems, an external server is recommended to aggregate the messages.

For session log messages, you can:

- Purge the contents of a log file – manually or automatically, based on a schedule you determine. For automatic purges, you can email copies of purged messages to an administrator. We recommended that copies of the messages be sent to an outside syslog consolidation server.

To configure session logs, select **Configuration, Logs**. Expand **Logs** to see the configuration choices.

#### **NOTE**

Session log files contain the IP address of the device requesting access. If your server is behind a networking device, such as a proxy, load balancer, or router, verify that the device prevents against IP spoofing of the X-Forwarded-For HTTP header.

- Save the log files as reports. If necessary, you can download these reports. For information viewing session logs and create reports, see [Session Management](#).

### Syslog for System Operation

The syslog provides comprehensive information about system operation, down to the component level. The syslog data is written to a text file. To configure syslog, select **Configuration, Logs, Syslog**.

Syslog-based activities include:

- User logins and logouts
- User requests for resources
- Violations
- Alerts
- System information

For syslog messages, save logs to an external server. Logs are saved in a comma-separated value (CSV) file format, which can be imported to spreadsheets and other applications. Reporting can be performed at the syslog level. Alternatively, a security information management tool can collect the syslog messages. When clustering is used, events are not consolidated.

### WARNING

To save syslog data to a log, configure a remote syslog server. Otherwise, the syslog records are not saved.

## Purge Session Logs Automatically

Use the automatic log purge feature to schedule the ongoing emailing and purging of logs. You can automatically purge logs from the database at a specified interval, between one hour and 120 days. An email containing a copy of the deleted logs can be sent to the administrator for long-term storage.

To save and purge log entries on demand, use [Save or Purge Session Logs Manually](#).

### NOTE

**Prerequisite:** The email account that is configured in **Configuration, Monitor** is the recipient of the log email. To receive an email, you must configure the email settings in the Monitor fields **Admin Email**, **SMTP Server**, and **Appliance From Address**. For instructions, see [Set Up Email for Monitoring](#).

Follow these steps:

1. Go to **Configuration, Logs, Automatic Log Purge**.
2. Select the **Enable as scheduled below** checkbox to turn on automatic purging.
3. Select the **Purge Interval** from the list of defined intervals. This number determines the frequency that logs are deleted.
4. Select the **Require Email Be Sent Before Purge** checkbox to send an email containing a copy of the deleted logs to the administrator.  
Messages in the body of the email are separated by carriage returns.
5. Select the **Email Size** (1 MB to 10 MB) to correspond to limitations of your SMTP server.  
If the log is larger than the email, the email is divided into multiple emails.
6. Select **Purge All Members in This Site** to purge the session logs from all the cluster members in this cluster site.

### NOTE

In a primary site, session logs are replicated among the site members, but in secondary sites, session logs are not. When you select this option in a primary site, one member purges sessions logs. Then the purge action (not the selected option) is replicated to other primary site members. In a secondary site, selecting the option replicates the selection and directs each site member to purge its own session logs.

7. Select **Update** to save your settings.  
If you change your settings without updating them, you can return to the previous settings by selecting **Reset**. This action does not return the settings to a default.

## Save or Purge Session Logs Manually

Automatic log purges are the recommended method of deleting logs. However, begin with a manual log purge. For a manual log purge, the best practice is to save, purge, download, and then delete the logs.



**Follow these steps:**

1. Go to **Configuration, Logs, Manual Log Purge**.
2. Use the **Until** calendar to specify a date up to which logs are saved or purged. The date is inclusive, so the logs from that date are also saved or purged.
3. Select **Purge All Members in This Site** to purge the session logs from all the cluster members in this cluster site.
4. Save the logs to a temporary file on the server by selecting **Save to File**.  
The logs are saved in a CSV file that is named with the end date you specified. The file is listed on the **Download/Delete Log Files** tab.
5. Purge the logs by clicking **Purge**.  
The logs are purged up to and including the specified date.
6. Download the saved file to your local computer. Go to the **Download/Delete Log Files** tab, select the file, and select **Download**.
7. To delete the CSV file from the server now that it exists locally, select **Delete** on the **Download/Delete Log Files** tab.  
This action frees up space on the server.

To purge all logs without saving them, select **Purge All** at the bottom of the page. We do not recommend this action.

## Configure an External MySQL Database for Session Logs (Optional)

You can configure an external MySQL database to store session logs. A copy of the log files is automatically kept on the local server in an internal database.

### NOTE

These procedures apply only to session logs; not to syslog messages.

### Configuring User Privileges for your MySQL Database

The user for the MySQL database where PAM stores session logs must have the following privileges:

- SELECT
- INSERT
- UPDATE
- DELETE
- CREATE
- REFERENCES

The following example procedures describe how to create a database, and then create a user with the appropriate privileges. Your actual procedures may be different based on your environment.

### **Follow these steps to create a MySQL database and a user with the correct access rights:**

1. As the user `root` or as a database administrator, run the following command to create the database where PAM should store the session logs:

```
create database <db_name> DEFAULT CHARACTER SET utf8mb4 DEFAULT COLLATE utf8mb4_unicode_ci;
```

Where `<db_name>` is the name of the database you are creating.

2. Run the following command to create the DB user that PAM uses to access this database:

```
create user '<db_username>'@'%' IDENTIFIED WITH mysql_native_password BY '<db_password>';
```

Where:

- `<db_username>` is the name of the database user you are creating.
  - `<db_password>` is the password for the database user you are creating.
3. Run the following two commands to grant the database user the SELECT, INSERT, UPDATE, DELETE, CREATE, and REFERENCES privileges on the database that you created:



```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, REFERENCES ON <db_name>.* TO <db_username>@'%';
FLUSH PRIVILEGES;
```

Where:

- <db\_name> is the name of the database
  - <db\_username> is the name of the database user
4. if you are using MySQL version 8:
    - a. Edit the MySQL configuration file. Under [mysqld], change the default\_authentication\_plugin to mysql\_native\_password.
    - b. Restart MySQL

## Configuring PAM to Recognize your MySQL Database

Follow these steps to configure PAM to recognize your PAM Server:

1. Go to **Configuration, Logs, External Log Server**.
2. Select the **Enable logging to the external server** checkbox.
3. Select **local** or **external** for which logs are shown by default.
4. To allow regular users to change the view from **local** to **external**, select the **Allow user to change view** checkbox.
5. For the MySQL server settings, complete the following fields:
  - **Server:** Enter the IPv4 or IPv6 address of the MySQL server.
  - **Port:** By default the port is 3306, otherwise, enter the port number.
  - **DB Username:** Specify a user with SELECT, INSERT, UPDATE, DELETE, CREATE, and REFERENCES privileges to the database.
  - **DB Password:** Enter the password for the database user.
  - **Database Name:** Enter the name of the database.
6. Click **Update** to save your settings and activate external logging.

If you change your settings, but you do not update them, you can return to the previous settings by selecting **Reset**. This action does not return the settings to a default.

## Configure a Splunk Server for Logging

A Splunk server works with the PAM appliance to monitor logs. Splunk collects information from the application code, and then sends data as key/value pairs. This format makes the information easier to consume, such as in reports or on dashboards.

PAM forwards logs to Splunk servers using a logstash component that runs inside a docker container. This mechanism allows PAM to support more options to connect to Splunk servers, along with two additional formats, Space Delimited and JSON, for the audit and metric log messages. These new options are available immediately with a fresh installation.

### NOTE

Deployments with Splunk servers configured prior to **upgrading** to PAM 4.0.2 (or later) can preserve their legacy Splunk configuration to support backward compatibility. This is called legacy Splunk mode. Users that upgrade to 4.0.2 but do **not** have any Splunk servers currently configured use the new functionality. Such users will not see the **Use Legacy Splunk Mode** option.

In legacy Splunk mode, Splunk Forwarder 6.2 (instead of the new logstash) forwards the logs to the Splunk servers. The legacy Splunk mode has limited connectivity options, and only supports the TCP protocol.

Depending on your PAM version and current Splunk server configuration, have three options to configure your Splunk server. You can also configure your Splunk server as a Syslog server.

## Configure Splunk Servers

Use these steps to add or configure Splunk servers.

### Follow these steps:

1. Go to **Configuration, 3rd Party, Splunk**. The default display shows the **Splunk Servers** tab. This tab displays, if any, the currently-configured Splunk server name, access port, security protocol, and whether the Splunk server uses Transport Layer Security (TLS).
2. Select **Add**.  
The **Add Splunk Server Configuration** screen appears.
3. In the **Address** field, enter either the Splunk server IP address or Fully Qualified Domain Name (FQDN). For FQDN, the DNS must be set up properly on the **Configuration, Network, Network Settings** page. A specified FQDN can be no longer than 255 characters.
4. Enter the **Port** to use on the Splunk server.

#### NOTE

Configure the port on the Splunk server by selecting **Settings, Data Inputs**. Depending on the protocol to configure(TCP / UDP), select **Add New**.

5. Select the desired **Protocol** to use: **TCP** or **UDP**. If you select **TCP**, the **Enable TLS** option becomes available.
6. Select **Enable TLS** to ensure that data is sent over a secure communication channel.

#### NOTE

If you want to use the **Enable TLS** feature with PAM, make sure to configure TLS on the Splunk server as well.

7. Select the **Test** button before saving this information to assess if the Splunk configuration is correct. A message appears to remind you to check the Splunk server to verify that the test message appears on the Splunk server.

#### NOTE

The **Test** button does not verify the configuration by itself. Selecting the **Test** button means PAM sends a test log message to the address and port number of the Splunk server. You must check the Splunk server to verify if the message was received.

8. Select **OK** to save and exit this window.
9. Repeat for each server.
10. Use the **Update** button to edit a selected server in the Server list.
11. Select the **Splunk Settings** tab.
12. Select the format to send messages to Splunk servers from the **Message Format** drop-down list: **XML** (the default), **Space Delimited**, or **JSON**.

#### NOTE

The **Message Format** *ONLY* applies to the audit and metric logs.

Selecting **Update** on the **Splunk Settings** tab affects all currently-configured Splunk servers. You do not have to select the message format for each Splunk server.

13. Select **Update** to commit your selection.

#### NOTE

After saving the configuration, the system requires a few seconds for the logstash service to start, and for the server to receive the logs.

## Configure Splunk as a Syslog Server

A second option is to configure your Splunk server as a Syslog server. Syslog sends data on UDP port 514 by default. You can change this port to match your Splunk Receive Data port setting. Syslog is configured from the **Configuration, Logs, Syslog** page. See [Configure a Remote Syslog Server](#) for more information.

## **Configure Legacy Splunk Servers**

Follow these steps to configure or maintain your legacy Splunk configuration. On the **Splunk Settings** tab, the **Use legacy Splunk mode** option is enabled to indicate that you are in legacy mode. Note that the Legacy Splunk mode has limited Connectivity options, and only supports the TCP protocol.

### **Follow these steps:**

1. Go to **Configuration, 3rd Party, Splunk**.
2. Select **Add**.  
The **Add Splunk Server Configuration** window appears.
3. Enter the Splunk server IP address and port in the appropriate fields. For the **Address**, enter either the Splunk server IP address or Fully Qualified Domain Name (FQDN). For FQDN, the DNS must be set up properly on the **Configuration, Network, Network Settings** page. A specified FQDN can be no longer than 255 characters.  
**Note:** The port is configurable in Splunk, under **Settings, Forwarding and Receiving, Receive Data**.
4. Select **OK**.
5. Repeat for each server.
6. Use the **Update** button to edit a selected server in the Server list.

## **Migrate Legacy Splunk Servers**

Follow these steps to migrate your legacy Splunk servers to the new Splunk configuration. Upon successful migration, all existing server configurations will be used by Logstash inside PAM to forward logs to Splunk servers.

### **NOTE**

Be advised that you cannot reverse the migration. A warning message appears prompting you to confirm the migration. After this migration, you must reconfigure the Splunk server to ensure all logs get forwarded without any issues. Your Splunk server list in PAM does not require reconfiguration.

### **Follow these steps to migrate legacy Splunk servers:**

1. Go to **Configuration, 3rd Party, Splunk**.
2. Select the **Splunk Settings** tab.
3. Clear the **Use Legacy Splunk Mode** option.
4. Select **Update**.
5. In the message that appears, confirm that you want to disable legacy mode.

### **NOTE**

After you have disabled legacy mode, refer to the following section named [Configure New Splunk Servers](#) for more information.

## **Configure a Remote Syslog Server**

You can configure external Syslog servers to receive and save syslog events. You must configure a remote syslog server to save syslog records.

### **Follow these steps:**

1. Go to **Configuration, Logs, Syslog**.
2. Set the **Syslog Enabled** option.
3. From the **Message Format** drop-down list choose one of the following formatting options for messages that are sent to the Syslog servers:
  - **XML** (the default)
  - **Space Delimited**
  - **JSON**

**NOTE**

The specified **Message Format** *only* applies to the audit and metric logs. For more information, see [Syslog Message Formats](#).

4. Select the **Add Server** button (blue with a white plus sign) to add a new syslog server. A new row appears in the table.
5. In the **Server** column field, enter either the server IP address or Fully Qualified Domain Name (FQDN).
6. Optionally, specify a **Port** value for the remote syslog server. If you leave the port blank, it defaults to 514.
7. Select the desired **Protocol** to use: **TCP** or **UDP**. If you select **TCP**, the **TLS** option becomes available.
8. Optionally, select **TLS** to ensure that data is sent over a secure communication channel.

**NOTE**

If you want to use the **Enable TLS** feature with PAM, make sure to configure TLS on the Syslog server as well.

9. Select **Update** to save your settings and activate the servers.

**NOTE**

After saving the configuration, the system requires a few seconds for the logstash service to start, and for the server to receive the logs.

If you change your settings, but you do not update them, return to the previous settings by selecting **Reset**. This action does not return the settings to a default.

## Configure a Server Control User Activity Server

You can configure up to two external logging servers for Server Control Utility Appliances to receive and save user activity log events. You must configure a remote logging server to save Server Control user activity log records.

### Follow these steps:

1. Go to **Configuration, Logs, Server Control User Activity**.
2. Select the **Enable Event Forwarder** checkbox to send PAM Server Control user activity log events to the remote server.

**NOTE**

The **Event Forwarder** service uses the TCP protocol to forward the events to an external SIEM server (for example, splunk). Therefore, make sure to configure the SIEM server to listen over TCP.

3. In the **Primary Server** text box, enter either the server IP address or Fully Qualified Domain Name (FQDN) of the primary server.

**NOTE**

You can use a FQDN for the remote logging server if the Utility Appliance can resolve the domain name. If not, you must use the IP address instead.

4. In the **Failover Server** text box, enter either the server IP address or Fully Qualified Domain Name (FQDN) if the backup server takes over if the primary server fails.
5. Specify a **Remote Port** value for the remote server. If you configure two remote server destinations, both must use the same port.
6. Select **Update** to save your settings and activate the servers.

**WARNING**

If you change the **Port** value, you must do one of the following procedures after applying that change (as appropriate for your environment):

- **Standalone appliance:** Restart the appliance.
- **Clustered environment:**
  - a. Stop the cluster.

- b. Restart each node that is connected to a remote server.
- c. Start the cluster.

If you change your settings, but you do not update them, return to the previous settings by selecting **Reset**. This action does not return the settings to a default.

### WARNING

If one or more Server Control Utility Appliances are present in your deployment, any updates made on the Server Control User Activity config in PAM will get propagated to all Utility Groups. In a PAM cluster, any PAM node can overwrite the previously configured Event Forwarder that has been used by the Utility Groups.

## Troubleshoot User Interface Problems

As an administrator, you can capture logs from user interface interactions to help troubleshoot problems. You should only undertake these steps with the help of Broadcom Support.

### User Interface Activity

The user interface generates many messages, which the UI Logging captures as log entries. At the "Debug" level, each user can generate hundreds of entries logging in, hundreds of entries per minute, and thousands per day. UI logging is only done for one individual user at a time.

### NOTE

In clustered environments, UI logging is not supported on Secondary sites. A cluster user on a Secondary site must recreate the UI problem on a Primary site.

Example of UI Log entries:

```
Date,Username,ClientIP,LogLevel,Detail
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.main.MainGlobals.getConfigurationOptionValue() - configuration option
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.main.MainMenu.createMenuItems() - Menu item not visible for Devices
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.SystemGlobals.hideGlobalMask() called maskRequestCount = 1
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.NavigationManager.initializeNavigationManager() - Performing first setup
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.store.common.FilterView.afterLoadCallback() - successfully loaded 1 records
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.store.users.LoggedInUser.afterLoadCallback() - successfully loaded 1 records
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.SystemGlobals.hideGlobalMask() - hiding mask since no more requests!
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.SystemGlobals.showGlobalMask() called for first time!
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.main.MainGlobals.loadStores() - Starting load of global discovery stores
2018-02-01 16:51:30.0,standard,10.1.7.7,DEBUG,CA-
PAM.view.common.main.MainGlobals.loadConfigurationOptions() - Starting load of feature
```

## **Troubleshooting Example**

A user has an issue that is related to the user interface, and contacts an administrator. The administrator is unable to solve the problem, and contacts Broadcom Support. The support engineer assists the administrator in taking these steps:

1. If you are using a Multi-Site cluster, determine whether the user is logged on to a Primary or Secondary site member.
2. Request that the user log out from Privileged Access Manager.
3. The administrator logs in. If it is a cluster, log in to the Primary site.
4. Purge any UI logs.
5. Enable UI logging. The UI Log option only appears on the Primary site of a cluster.
6. The user must then log in again to the Primary site.
7. The user should repeat the actions that led to the issue.
8. Request that the user logout.
9. Disable UI Logging.
10. Inspect the UI Log entries. Look for errors, configuration problems, or other clues suggested by the specific user experience.

## **Enable UI Logging**

UI Logs can only be enabled for one user at a time. This user must already exist as a Session Manager User.

### **Follow these steps:**

1. Go to **Configuration, Diagnostics, UI Log**.  
The **UI Log Settings** tab appears.
2. Select the **Enable UI Logging** checkbox.
3. To select a **UI Logging User**, click the Select magnifying glass icon. The **Session Manager Users** dialog appears. Select a User and click **OK**.

### **NOTE**

The administrator can only enable UI logging on the Primary site of a cluster. The user must then log in again to the Primary site to recreate the issue.

4. Select the **Log Level**.
  - **Error** saves Error messages only.
  - **Info** saves Error and Info messages.
  - **Debug** saves Error, Info, and Debug messages.
5. The **Log Purge Interval** is how often the purge runs, in hours. **Log Purge Retention** is how much log data to retain, from one to seven days. For example, the default interval is hourly, and the default retention is daily. If enabled, this configuration keeps data for the most recent 24 hours, deleting anything older than that every hour. Therefore, you would always have from 24 through 25 hours of the most recent data.
6. Click **Save** to save your settings and activate UI logging.

## **Inspect Log Entries**

The second tab on the UI Log page is **UI Log Entries**. This tab is the only place to view the UI log entries, although you can download them. The entries are logged in the database, and can be downloaded as a CSV file.

### ***Filter***

You can filter the entries that are displayed using the **Column** and **Value** fields, and clicking **Filter**.

- You can combine filters by selecting **Add Filter** and selecting multiple **Column** and **Value** combinations.
- To search on a date and time range, use the **Start Timestamp** and **End Timestamp Columns**.
- The **Message** column Value accepts \* (asterisk) as wildcards. You can use \_ (underscore) as a single character wildcard.  
*For example, filtering on \*config\* can return changed configuration settings.*
- The **Reset** button removes all filters and displays all log entries.

### View

The **View** button displays the details for a selected (highlighted) log entry. Double-click the entry for the same result.

### Download

The **Download** button downloads the log entries to a CSV file on your local computer. If a **Filter** is active, only the results are downloaded.

### Purge All

The **Purge All** button deletes *all* log entries immediately.

## Diagnostics and Troubleshooting

The Privileged Access Manager Diagnostics page is available from the Configuration menu. The information that is collected there is used for Broadcom Support analysis of Privileged Access Manager operation.

### NOTE

When preparing a diagnostics package, use these functions only under the direction of Broadcom Support.

### Next Steps

- [Configure Diagnostic Logs](#)
- [Configure Performance Graphs](#)
- [Configure System Diagnostics, Maintenance, and Cluster Tuning Options](#)
- [Tools](#)

## Configure and Obtain Diagnostic Logs

Use the **Diagnostic Logs** pane (**Configuration, Diagnostic Logs**) to configure the detail level of and obtain diagnostic logs that are required to analyze issues with your environment.

### IMPORTANT

The **Diagnostic Logs** pane is intended for use when working with Broadcom Support to access diagnostic logs that they require to analyze issues with your environment. Only log levels if you are instructed to do so.

The **Diagnostic Logs** panel contains the following tabs:

- **Log Levels** tab: Change the detail level of diagnostic information that is collected by a particular log or logs, then select the **Submit** button to commit your changes. Otherwise, leave the default values.

### WARNING

Log files can grow rapidly if you set their log level to a more detailed value. Restore them to a lower level when the higher level is no longer required. To monitor disk usage, select **System Info** at the top of the PAM UI. If it is too high, reboot the PAM server to clear the logs.

- **Download** tab: Access recent log entries or download complete log files from the PAM server to your local system so that you can send them to Broadcom Support for diagnostic inspection.

The following sections describe how to set the detail level of and download log files, as applicable.

### Set the Detail Level of and Access the Tomcat Log

The Tomcat `catalina.out` log file is used to diagnose Credential Manager issues.

To change the detail level of the Tomcat log, open the **Log Levels** tab and select the required value from the **Tomcat Log Level** drop-down menu.

**Values:** "Severe" "Warning" (the default), "Info", "Config", "Fine", "Finer", "Finest", and "off"

To see recent unfiltered log entries from the Tomcat log in a dialog, open the **Download** tab and select the corresponding **Recent Log Entries** button. To download the `catalina.out` file, select the associated **Download** button.

### ***Access the Internal Connector Framework Log***

To view recent unfiltered Internal Connector Framework log entries, open the **Download** tab and select the associated **Recent Log Entries** button. To download the Internal Connector Framework log file, select the associated **Download** button.

### ***Set the Detail Level of and Access the Symantec PAM as SAML RP Log***

To change the detail level of the Symantec PAM as SAML RP log, open the **Log Levels** tab and select the required value from the corresponding drop-down menu.

**Values:** "Normal" (the default) or "Verbose"

To see recent unfiltered log entries from the Symantec PAM as SAML RP log, open the **Download** tab and select the corresponding **Recent Log Entries** button.

### ***Set the Detail Level of and Access the Symantec PAM as SAML IdP Log***

To change the detail level of the Symantec PAM as SAML IdP log, open the **Log Levels** tab and select the required value from the **Symantec PAM as SAML IdP Log Level** drop-down menu.

**Values:** "Normal" (the default) or "Verbose"

To see recent unfiltered log entries from the Symantec PAM as SAML IdP log, open the **Download** tab and select the corresponding **Recent Log Entries** button.

### ***Set the Detail Level of the Web Services Log***

To change the detail level of the Web Services log, open the **Log Levels** tab and select the required value from the **Web Services Log Level** drop-down menu.

**Values:** "Error" (the default), "Warning", or "Debug"

### ***Set the Detail Level of the Utility Orchestrator Log***

To change the detail level of the Utility Orchestrator log, open the **Log Levels** tab and select the required value from the **Utility Orchestrator Log Level** drop-down menu.

**Values:** "Off", "Error", "Warning", "Info", "Debug" (the default), or "Trace"

### ***Set the Detail Level of the LDAP Sync Log***

To change the detail level of the LDAP Sync log, open the **Log Levels** tab and select the required value from the **LDAP Sync Log Level** drop-down menu.

**Values:** "Normal" (the default) or "Verbose"

### ***Set the Detail Level of the Applet Log***

To change the detail level of the applet logs, open the **Log Levels** tab and select the required value from the **Applet Log Level** drop-down menu.



**Values:** "Error", "Warning", "Info", "Debug" The default is "Error".

**NOTE**

The specified value is replicated to all cluster members.

### ***Enter Applet Debugging Commands***

If Broadcom Support provides you with applet debugging commands, open the **Log Levels** tab and enter the commands in the **Applet Debugging** field. If there are multiple commands, enter them as a comma-delimited list.

**NOTE**

The specified commands are replicated to all cluster members.

### ***Download System Diagnostics Files***

To download system diagnostics files, open the **Download** tab and use the following **System Diagnostics Files** options (as applicable):

- If Broadcom Support asks you to change the number of days of system diagnostics files to download, use the **Past Days** field. (Range: 1 to 30; default: 14). Set the **All Logs** option to specify that the download should include all available days.
- Select the **Download** button to save the files to your local system.

**NOTE**

If core dumps are being collected, they are included in the system diagnostics download.

### ***Use a System Log Configuration File to Specify Multiple Log Files to Download***

To download multiple log files that are specified in a System Log Configuration File provided Broadcom Support, do the following steps using the **System Log Configuration File** controls on the **Log Levels** tab:

1. Select the **Choose File** button.
2. In the **File Upload** panel that opens, locate the System Log Configuration File on the local drive and select **Open** to upload it into PAM.
3. Select **Download** to download specified log files.

### ***Set the Detail Level of and Download SPFD (Secure Port Forwarding Daemon) Logs***

To change the detail level of the SPFD and WolfSSL logs, open the **Log Levels** tab and select the required value from the **SPFD Log Level** drop-down menu.

- **Info** (Default): Only info-level events are included in the SPFD and WolfSSL logs.
- **Debug**: Debug-level events are included in the SPFD log; Only info-level events are included in the WolfSSL log.
- **Info+WolfSSL**: Only info-level events are included in the SPFD log; Debug-level events are included in the WolfSSL log.
- **Debug+WolfSSL**: Debug-level events are included in the SPFD and WolfSSL logs.

To download the SPFD log for the service provider daemon to your local system, open the **Download** tab and select the corresponding **Download** button.

### ***Download Analytics Logs***

To download analytics logs to your local system, open the **Download** tab and select the corresponding **Download** button.

### ***Download Service Desk Logs***

To download service desk logs to help troubleshoot issues with an integrated [service desk solution](#), select the corresponding **Download** button.

## Configure Performance Graphs

Privileged Access Manager activity can be graphed by turning on Performance Graphs. Follow these steps:

1. Go to **Configuration, Diagnostics, Performance Graphs**.
2. Select **On**, then select **Submit**.  
Graphics can take 20 minutes to be displayed. The following dimensions are displayed:
  - a. **CPU Utilization**
  - b. **Outgoing Network Activity DD/MM/YYYY**
  - c. **Incoming Network Activity DD/MM/YYYY**

## Configure System Diagnostics, Maintenance, and Cluster Tuning Options

You can configure the following functions on the **Configuration, Diagnostics, System** page:

- system diagnostics
- maintenance options
- cluster tuning options

After enabling or disabling any modes, select the **Submit** button.

### System Diagnostics Options

Use the following system diagnostics options in coordination with Broadcom Support to allow them to analyze and troubleshoot the operation of your PAM environment.

#### **Enable AACTRL Debug Mode**

Set the **AACTRL Debug Mode** option (on the **Modes** tab) only if instructed to do so by Broadcom Support.

#### **Enable Remote Debugging Services**

The **Remote PAM Debugging Services** mode lets Broadcom Support access your appliance for debugging purposes. Enable this mode only at the instruction of Broadcom Support. Otherwise, keep this setting turned off.

If you enable Remote PAM Debugging Services, be aware of the following information:

- If you upgraded from PAM 3.2 with debugging enabled, the expiration date is automatically set to 30 days from the current date and time. You can update this expiration date.
- If you activate FIPS mode when Remote PAM Debugging Services mode is on, the service setting is turned off. If necessary, return to this screen and set this mode back on.
- If PAM is operating in FIPS mode and you set **Remote PAM Debugging Services** on, rebooting the appliance turns off the setting. If necessary, return to this screen and set this mode back on.

#### **Follow these steps:**

1. Select **Configuration, Diagnostics, System**.
2. For Remote Debugging Services, Select **On**. When you select On, an expiration date and time appears that is seven days from the current date and time.
3. To change the expiration date for access to these services, select **Until**. Select a date and time from the calendar and time selection drop-down list.
4. When your changes are complete, select **Submit**.

#### **Run System Diagnostics**

Use the System Diagnostic tool (on the **Download** tab) to gather information about specific file versions. The tool provides a listing of file names, showing the dates that they were modified and their file versions. To run the system diagnostic, follow these steps:

1. Obtain a configuration file from Broadcom Support.
2. Save the file in a location accessible to the appliance.
3. Go to the **Download** tab on the **Configuration, Diagnostics, System** page.
4. Select **Choose File** to access the configuration file.
5. Select **Run System Diagnostic**.  
The system downloads the result in the diagnostic.enc file.
6. Follow any further instructions from Broadcom Support.

### ***Activate the System Monitor Tool***

Select the **Activate System Monitor** button (on the **Download** tab) to obtain encrypted output of system diagnostics information.

## **Maintenance and Cluster Tuning Options**

Use the following options to enable maintenance mode and cluster tuning.

### ***Enable Maintenance Mode***

Enable the **Maintenance Mode** option (on the **Modes** tab) to prevent new user logins so that an administrator can perform configuration changes. These changes might otherwise disrupt or be disrupted by user activity. In Maintenance Mode, when a user who is not a Global Administrator tries to log in to the appliance, the user sees an error message: "This Privileged Access Manager is in maintenance mode. Only admin level users can log in."

The following conditions also apply in Maintenance Mode:

- Prevents new, scheduled jobs from running
- Prevents non-administrative users from logging in. To log in, a user role requires the privilege "configurationManage."
- The internal load balancer for the appliance does not send traffic to a node in maintenance mode. If all cluster members are in maintenance mode, traffic is still routed to one of the members. However, only a PAM administrator can log in.

### **NOTE**

Although new logins are prevented, current user logins are not disconnected at the time Maintenance Mode is set. The administrator might, for example, send an email requesting currently connected users log out, or when necessary, force disconnections through the **Sessions, Manage Sessions** interface.

Maintenance Mode does not disable the Credential Manager CLI.

### **To disable the Credential Manager CLI, follow these steps:**

1. Go to **Configuration, Security, Access**.
2. On the **Access** tab, select Disabled for **Credential Manager CLI**.
3. Save the change.
4. If necessary, restart the appliance.

### ***Enable Cluster Tuning Mode***

Enable the **Cluster Tuning Mode** option (on the Modes tab) to enable you to alter default settings for a cluster. If **Cluster Tuning Mode** is enabled, the tuning settings are found on the **Cluster Tuning** tab of the **Clustering Configuration** page. Certain of those settings should only be changed in consultation with Broadcom Support.

See [Set Up a Cluster](#) for more information about clustering, and [Cluster Tuning](#) for specifics about these settings.

## Networking Tools

The Networking Tools page (**Configuration, Tools**) provides network diagnostic tools. Use these tools to check device connectivity and troubleshoot communication from the Privileged Access Manager appliance. Test networking with the standard ping, traceroute, DNS resolution, and port scan. These settings define attributes to provisioned objects such as Users, Devices, and passwords, but are not derived from, or attached to any specific objects.

### *Ping*

Enter an IP address and select the **Ping** button to initiate an ICMP echo to the device associated with that address. The Ping Result window appears with ping statistics.

### *Traceroute*

Enter an IP address and select the **Traceroute** button to identify a network route from Privileged Access Manager to the device with that address. The Traceroute Result window appears with route trace results.

### *Resolve Name*

Enter a hostname and select the **Resolve Name** button to determine the IP address of that host. The Name Resolve Result window appears with the IP address result.

### *Port Scan*

No default range of ports is assumed for the Ports field. You must enter your desired port scan range. Use a comma between ports or a dash to specify a range of ports. You can combine these methods, for example: 22,23,45-1024. Do not insert spaces.

1. In the **IP Address** field, enter the target IP address for the port scan.
2. In the **Ports** field, enter the range of ports you want to scan.  
Commonly used ports:  
HTTP 80  
HTTPS 443  
RDP 3389  
SSH 22
3. In the **Timeout** field, enter a desired timeout in minutes.
4. Press the **Port Scan** button to initiate a scan of open ports on the device that is associated with that address.  
The Port Scan Result window appears with the port type, status, and service

### *Bulk Network Scan*

When enabled from [Global Settings](#), the Bulk Network Scan tool allows Administrators to run a bulk scan of their network (Host/Port) to determine the status of ports (open/filtered).

Bulk Network Scans are invoked by uploading a CVS file where each line is of the following format:

```
IP address, Port, Options
```

Both the IP Address and the Port fields can accept ranged values (example: 10.17.43.1/24,21-100). Options can be any valid nmap options except -oX, -oN, -oG, -oS, -oA, -iL (example: -n -T4 -sT -PN --max-scan-delay 0ms).

A Bulk Network Scan runs locally on the PAM node it is initiated from, so progress and results can only be checked on the same PAM node.

Only one Bulk Network Scan can be initiated on a PAM node at a time. Starting a new Bulk Network Scan after one has completed overwrites the results of the previous scan.

The maximum size of the CVS input file for a Bulk Network Scan must not exceed 1 MB. The file that results from the scan that you download is limited to 10 MB.

To run a Bulk Network Scan, follow these steps:

1. Select the **Download Sample File** link.
2. Prepare the CVS file.
3. Select **Start Scan**. The scan progress bar shows the status of the scan. You have the option to cancel the scan at any time. You can navigate away from this page and return at any time.
4. When the scan is complete, the **Download Results** button activates. The results are delivered as a CVS file compressed with gzip.
5. To start a new scan, select a new file and choose **Start Scan**.

## Set Up Email for Monitoring (Legacy)

Configure the general monitor parameters that Privileged Access Manager uses to send alert emails.

### NOTE

DNS must be configured in **Configuration, Network**, and working for the monitoring function to run.

To set these parameters, follow these steps:

1. Go to **Configuration, Monitor (Legacy)**.
2. Enter an email address for the Privileged Access Manager administrator in **Admin Email**. Consider a role account to allow multiple recipients.
3. Enter the **SMTP Server** as an IPv4 address, an IPv6 address, or an FQDN host. (For IPv6 addresses, enclose the IP with square brackets.)
4. Enter a valid email address as the **Appliance From Address**. This address appears as the "From" field of any Privileged Access Manager monitoring email.  
**Note:** A trailing or leading space also causes an error.
5. Select a value, in seconds for the **Re-check Time** to check for alerts.
6. Enter an FQDN in **DNS Test Query** to test that DNS is available and operating correctly.
7. To start the monitor, select the **Monitor** tab.
  - a. Select **Start at boot** to start the monitor when Privileged Access Manager boots up. Select **Save** to save that setting.
  - b. Select **Start** to start the monitor immediately.
  - c. Select **Stop** to stop the monitor immediately.

The read-only **Running** checkbox indicates whether the monitor is running.

## Microsoft Office 365 Configuration

Privileged Access Manager offers support for the protection of Microsoft online services to secure and audit privileged users accessing Microsoft Office 365. To connect to your Office 365 installation and configure Privileged Access Manager, follow these steps:

1. Go to **Configuration, 3rd Party, Microsoft Office 365**.
2. Enter your Office 365 configuration information:
  - a. Enter the **Security Token Service (STS) Endpoint URL**. In general, specify the appropriate URL that is exposed by your organization Active Directory Federation Service (ADFS). The endpoint must support the WS-Trust 2005 (username mixed mode) protocol.  
For example: `https://<ADFS Server FQDN>/adfs/services/trust/2005/usernamemixed`  
This value is user-supplied and might change.
  - b. Enter the **Security Token Service (STS) Endpoint Reference URI**. When ADFS is federated with Microsoft Online (MSOL), this value is typically:  
`urn:federation:MicrosoftOnline`

- c. Enter the **Microsoft Online Portal URL**. For example: <https://login.microsoftonline.com/login.srf>
- d. Enter the **Microsoft Online Portal Context Data**.
  - For Office 365 on Windows Server 2012 and later, ADFS 3.0 does not support "smart links." Make a connection to Office 365 from a browser and capture the entire URL string. You can use a product such as HTTP Analyzer or Fiddler to capture the string.
  - For earlier versions of Office 365, before ADFS 3.0, derive the value by "creating a smart link." Microsoft no longer supports or documents this procedure, but you can find smart link generators online.
3. Select **Save**.
4. Select **Ping** to test the information you entered.

## Power, Reboot, and FIPS Mode Controls

This content describes how to shut down or reboot a physical or virtual appliance instance. It also describes how to activate FIPS mode.

### Shut Down or Reboot a Physical Appliance

To shut down or reboot a physical appliance, navigate to the **Configuration, Power** pane in the PAM UI and select the corresponding option:

- **Power Off Appliance**: Shut down the appliance remotely. Note the following information
  - The power switch on the physical appliance remains in the ON position.
  - The **Configuration, Power** pane indicates that the appliance is shutting down but does not update.
- **Reboot Appliance**: Shut down then reboots the appliance remotely.

### Virtual Appliance Power Settings

To safely shut down or reboot a virtual appliance, navigate to the **Configuration, Power** pane in the PAM UI and select the corresponding option:

- **Stop Instance**
- **Reboot Instance**

If the PAM UI is not accessible, use the options for your platform:

- For Azure, use the **Start**, **Stop**, and **Restart** options from the Azure portal.
- For AWS and VMware instances, use the **Reboot** or **Power off** option on the PAM Utility Console.



### WARNING

If you are using the vSphere client, do not shut down the PAM instance using the Power Off option. Use the vSphere Power, Shutdown Guest OS, or Restart Guest OS option.

### Activate FIPS Mode

To implement FIPS encryption, complete the following procedures to enable FIPS mode on your PAM appliance.

### WARNING

After you activate FIPS mode, it cannot be undone.

### **Download the FIPS Software**

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

### **Activate FIPS**

### WARNING

- Before you activate FIPS mode for appliances in a cluster, turn off the cluster *first*. To turn off the cluster, navigate to **Configuration, Clustering**. Stopping or rebooting a cluster member requires cluster resynchronization.
- Ensure that you have access to the certificates that you have uploaded. You have to upload them again after activating FIPS.

After you install the PAM with FIPS, follow these steps:

1. If you are using PKI/Smart Card for user login, disable this feature:
  - a. Navigate to **Configuration, Security, Access**, and select the **PKI/Smart Card Options** tab.
  - b. Set the **PKI/SmartCard User Login** option to **Disabled**.
  - c. Select **Save**.

2. Navigate to **Configuration, Power** and select **Activate FIPS Mode**. The appliance reboots automatically after activation.

When PAM is rebooted from the UI, the message the following message displays:

"PAM appliance is rebooting... Please wait until the login screen appears ..."

After the appliance reboots, the UI login page is presented. When a reboot is initiated through a web browser, the login page might not display after the appliance reboots. If you are not returned to the login page automatically, refresh the browser or navigate to the login page by entering the URL for the UI.

3. To verify that FIPS is enabled, select **System Info** in the top-right corner of the UI. On the **Basic Info** tab, the FIPS Mode status should say Enabled.
4. After you enable FIPS mode, reload the certificates from the **Configuration, Security, Certificates** panel. See [Secure Connections Using SSL Certificates](#) for detailed instructions.
5. If you are using PKI/Smart Card for user login, re-enable the option on the **Configuration, Security, Access** panel.

### **Unavailable Configuration Options in FIPS Mode**

In FIPS mode, the following configuration options are not available:

- **Security, SAML, RP Configuration**, the Accept RSA-SHA1 Signed Responses option is hidden.
- **Security, SAML, RP Configuration, Configured Remote SAML IdP**, when you add an Identity Provider, RSA-SHA1 is disabled as a Signature Algorithm option.
- **Security, Access**, the TLS 1.0/1.1 Connection Allowed is disabled
- **Clustering** configuration, the **Generate Key** button is disabled.
- **SNMP** version 2c does not work. Use SNMP version 3 with FIPS Mode.

### **Upgrades and FIPS Mode Operation**

If PAM is already operating in FIPS mode, the appliance remains in FIPS mode after you upgrade to a newer release. If an upgrade impacts cryptographic operations relating to FIPS mode compliance, this information will be stated in the release notes.

Converting from commercial (Non-FIPS) to FIPS mode operation requires license changes. Contact your assigned Account Director for more details.

## **Configure Date/Time Settings**

This content describes how to configure Privileged Access Manager date and time settings which you access by selecting **Configuration, Date/Time**.

Change the date, time, and time zone configuration to set a new clock value.

### **WARNING**

Some processes that are running, such as SysInfo and Session Recordings, continue to use the previous clock value until the services are restarted. To ensure that all processes become synchronized after making a time change, reboot the system.

### **Set the Date and Time**

Modify the date and time settings for the Privileged Access Manager server using the controls on the **Date/Time** tab. The time settings implement the Network Time Protocol (NTP).

### **NOTE**

Each field in the **Date/Time** tab is static, reflecting the clock value at the time the page was opened. If you update the date and time manually, copy the time from a reliable source. Alternatively, use Time Servers.

To modify the date and time settings, enter accurate values in the **Date** and **Time** fields, and select **Update**.



## Specify Time Servers

To obtain the time from an NTP server, specify the time servers in the **Time Servers** tab. Some public servers are provided by default.

### NOTE

When you use a hostname rather than an IP address for an NTP server, ensure that a DNS server is configured. The DNS server ensures that the hostname resolves properly. Configure DNS Servers at **Configuration, Network, Network Settings**. See [Configure Network Settings](#) for details.

### Follow these steps:

1. To specify time servers, enter the fully qualified domain name of each time server you want to use to obtain the current time.
2. Optionally, select the **Synchronize at boot** check box to synchronize the time upon startup or a reboot the system.
3. Select **Save**.

If you are using NTP servers to set the time clock, you can configure NTP authentication so that the server can authenticate the time source.

## Configure the Use of Authenticated NTP

Configure the list of NTP servers in the **Authenticated NTP** tab.

### Follow these steps:

1. Paste the NTPv4 **Autokey** obtained from each NTP server into this section.
2. Select **Authentication Required** to use only authenticated NTP, and not communicate with unauthenticated peers.
3. Select **Save**.

## NTP Status

The **NTP Status** tab displays the status output from the NTP servers, in three parts:

### List of Time Servers

The first section is a list of time servers with a summary of the state of each server.

```

remote          refid          st t when poll reach  delay  offset  jitter
=====
+ntp.wdc1.us.lea 130.133.1.10    2 u  210 1024  377   43.580  -4.860  0.563
*ntp.your.org    .CDMA.          1 u  876 1024  337   25.847   1.148  0.148
-mtpbx.cytranet. 69.89.207.199   3 u   57 1024  377   44.839  -3.248  1.297
+linode.ibendit. 64.250.105.228  2 u  34m 1024  336   14.731  -3.632  0.444

```

The character in the left margin indicates time server status. This character is mapped to the value of the condition column in the Association Identifiers section.

Character	Condition	Description
space	reject	The peer is discarded as unreachable, synchronized to this server (sync loop), or outrageous synchronization distance.
x	falsesticker	The peer is discarded by the intersection algorithm as a <b>falsesticker</b> .

.	excess	The peer is discarded as not among the first ten peers, which are sorted by synchronization distance. This peer is probably a poor candidate for further consideration.
-	outlyer	The peer is discarded by the clustering algorithm as an <b>outlyer</b> .
+	candidate	The peer is a survivor and a candidate for the combining algorithm.
#	selected	The peer is a survivor, but not among the first six peers sorted by synchronization distance. If the association is ephemeral, it may be demobilized to conserve resources.
*	sys.peer	The peer has been declared the system peer and lends its variables to the system variables.
o	pps.peer	The peer has been declared the system peer and lends its variables to the system variables. However, the actual system synchronization is derived from a pulse-per-second (PPS) signal, either indirectly by the PPS reference clock driver or directly by kernel interface.

### Association Identifiers

The second section is a list of association identifiers for the server being queried, with **status** and **condition**. The **reach** column indicates the reachability of the server as **yes** or **no**. The **condition** column indicates its current state. The value `sys.peer` means that the time server is selected for use, while `candidate` means that the time server *can* be used.

```
ind assid status conf reach auth condition last_event cnt
=====
1 16746 943a yes yes none candidate sys_peer 3
2 16747 963a yes yes none sys.peer sys_peer 3
3 16748 9324 yes yes none outlyer reachable 2
4 16749 9424 yes yes none candidate reachable 2
```

### NTP Variables

The third section lists Privileged Access Manager NTP system variables in name-value pairs.

```
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.6p5@1.2349-o Fri Jul 22 17:30:51 UTC 2016 (1)",
processor="x86_64", system="Linux/3.16.39+pam02", leap=00, stratum=2,
precision=-21, rootdelay=25.847, rootdisp=45.240, refid=204.9.54.119,
reftime=de7a5190.7b075a77 Thu, Apr 12 2018 21:43:44.480,
clock=de7a54fc.a51301ea Thu, Apr 12 2018 21:58:20.644, peer=16747,
tc=10, mintc=3, offset=0.071, frequency=38.384, sys_jitter=2.650,
clk_jitter=0.498, clk_wander=0.055, host="gatekeeper", group="server",
flags=0x410001, digest="sha1", signature="sha1WithRSAEncryption",
update=201804010400, cert="gatekeeper gatekeeper 0x0",
```

until=201904010400

## Troubleshooting

If no record in the second section has value `sys.peer` in its **condition** column, then you do not have a good time server. Because time server synchronization takes time, you may need to select the **Refresh** button several times to get the latest status.

### NOTE

- [Apply Global Settings](#)
- [Apply Your Account Settings](#)

## Set Your Locale

Privileged Access Manager can be set to another locale instead of English. Setting a new locale changes the language of new messages and log data, but not the user interface. Existing data does not change. This change requires an appliance restart to take effect.

### NOTE

All members of a cluster must use the same locale. This setting applies to the back-end server data, not to client user interfaces.

**To change your locale, follow these steps:**

1. Go to **Configuration, Locale**.  
Your current locale is displayed in the **Locale** drop-down list.
2. To change your locale, select it from the drop-down list.
3. Select **Save**.  
The change takes effect when your appliance restarts.

## Change Your UI Language

The Locale setting changes data at the back end. To change the UI language in the PAM Client, see [Deploy the CA PAM Client](#). To change the UI language in a browser, change your settings.

**For example, in Internet Explorer 11, follow these steps:**

1. Select the **Tools** gear icon at the upper right.
2. Select **Internet Options**.
3. On the **General** tab, select the **Languages** button at the bottom of the window.
4. Select the **Language and input settings** button.  
The Language Preference window appears.
5. If your desired language is not listed, select the **Add** button. Find your language and select **OK**.  
**Note:** Some languages have multiple versions.
6. Once your desired language appears in the Language list, drag it to the top of the list, or use the **Move Up** button. Select **OK**.
7. Refresh the browser (select the **F5** key).  
Privileged Access Manager displays in the new language.
8. To change languages, repeat this procedure, moving your desired language to the top of the list. Select the **Remove** button to remove an unwanted language from the list.

**For example, in Internet Google Chrome, follow these steps:**

**NOTE**

Chrome is not supported for Access due to Java limitations, but functions well for administration and configuration.

1. Select **Settings** from the Chrome menu.
2. Select Advanced Settings and find the Languages heading.
3. Select the **Language and input settings** button.  
The Languages window appears.
4. If your desired language is not listed, select the **Add** button.  
**Note:** Some languages have multiple versions. Some cannot be displayed in Chrome.
5. Once your desired language appears in the **Languages** list, select the **Move to the top** option to make it the active language
6. Select the **Display Google Chrome in this language** button.  
If this button does not appear, use the **Add** button to find a different version of your desired language.
7. Select **Done**.  
Privileged Access Manager displays in the new language.

**Localized User Interface**

The Privileged Access Manager UI is optimized for localization.

When you access a target device or other remote entity with the localized product, the access method applets use the same language as the browser. However, the target device or any other remote device remains using the language in which it was installed. For example, a browser is set to Japanese. You launch the SSH applet to connect to a target device operating in English. The SSH terminal menu options are in Japanese but the command-line interface on the target device is in English. The locale of the target device determines the locale of the CLI.

## Configure Custom Branding

This procedure describes how to configure PAM to use your own logo in place of the Symantec logo in the PAM UI.

**Follow these steps:**

1. Go to **Settings, Branding**.
2. Use **Choose File** to select the logo graphics file. Only PNG files are accepted, with dimensions of approximately 55 x 55 pixels.
3. Select **Upload Custom Logo**.  
To use the original Symantec logo instead, select **Revert Logo**.

The uploaded custom logo affects only the logo on:

- The pre-login page on Internet Explorer 11
- The header bar after login

The uploaded custom logo does **not affect** the logo for the following components:

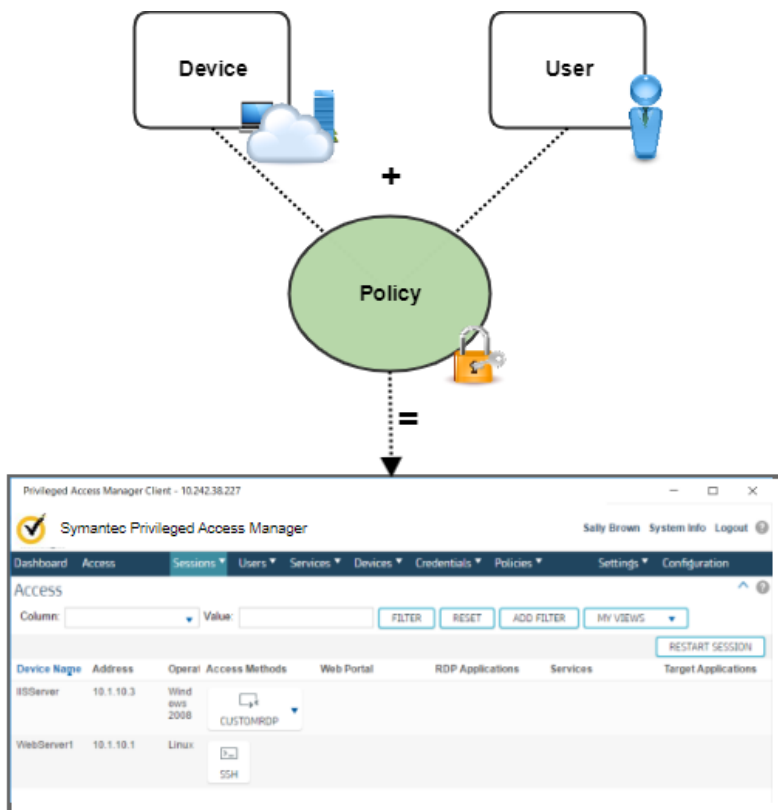
- The PAM Client
- The PAM Access Agent
- The text that appears after the logo

## Implementing Access Control

To configure PAM network-based access control, provision privileged access to devices and applications by configuring the following objects:

- **Devices** – Represent physical devices and IP-addressable applications.
- **Users** – Represent individuals who can log in to Privileged Access Manager.
- **Policies** – Define the relationships between users (or *user groups*) and *devices (or device groups)*, specifying what actions each user is permitted to do with each device.

In simplest terms, policies determine what device access options appear on the **Access** screen of each logged in user and whether their sessions are recorded.



This article describes these objects in more detail.

### Devices

A *device* object is a Privileged Access Manager-managed, IP-addressable network node that is the potential access *target* of a user. For example, a Windows or Linux system. You manage Devices from the **Devices, Manage Devices** screen in the UI.

When creating or importing devices, verify that the **Access** Device Type option is selected, or the device is not available in access policy selection lists.

**NOTE**

The **Password Management** and **A2A** device types are related to credential management. For more information, see [Protect Privileged Account Credentials](#).

**Access Types**

For each device, you specify one or more of the following *access types* to determine the ways in which it can be accessed:

- **Access Methods:** Prepackaged applets that provide standard connectivity
- **Services:** Configure services to extend the types of access beyond the predefined Access Methods to provide custom access to:
  - **TCP/UDP Services**
  - **RDP Applications**

**NOTE**

Access types that are configured at the device level determine all the possible access options available when configuring a policy involving that device. The access type or types that are presented to a *user* are specified in the corresponding access policy.

**Access Methods**

Access Methods are standard prepackaged Java communications applets that run in the PAM Client or a supported browser. Access Methods are available for VNC, TELNET, SSH, RDP, and serial connections. Access methods are predefined with standard ports and available to assign to devices out-of-the-box. To modify the default ports or disable Access Methods go to **Global Settings, Access Methods**.

**TCP/UDP Services**

Configure TCP/UDP Services to define custom access to known ports and to specific applications. These services may include fat client applications such as SQL query frontends, mainframe clients, or any proprietary application that uses a TCP or UDP connection. Web portals and web applications are also configured as Services.

Privileged Access Manager includes several preconfigured SFTP/FTP Services that support common SFTP/FTP servers including OpenSSH-derived Linux, AIX, Solaris SFTP, and Microsoft IIS implementations.

Configure other TCP/UDP Services (from **Services, TCP/UDP Services**) before configuring device definitions that require them.

**RDP Applications**

Define RDP Applications to provide access to RemoteApps – single target-hosted *applications that are published* through RDP protocol – instead of allowing access to the entire desktop.

Configure RDP Applications (from **Services, RDP Applications**) before configuring device definitions that require them.

**Device Groups**

For ease of administration, devices can be added and managed in groups. Devices in a *device group* are those which share common access methods and functionality, such as IIS Web Servers or UNIX and Linux variants. When using device groups, the concept of *deny* takes precedence: So, when selecting the access types available to a group, access types that are unavailable at the device level are not available at the group level. In other words, the most restrictive policy is used when a conflict arises.

When choosing Access Methods and Services for device groups, include *all* possible access methods and services for *all* devices in the group.

## Users

A *user* is a person who can log in to PAM. To simplify management, organize users in *user groups* for simplified management. Use *roles* to determine the permissions that a user has within Privileged Access Manager. User groups follow an inheritance model and roles can be assigned to groups and users.

### NOTE

[Credential Manager](#) has its own set of roles and user groups, separate from the roles and user groups defined for access.

### User Groups

User groups allow common sets of users to inherit the same role, authentication method, and other variables. User groups thus simplify management: a modification to the role for the group changes the role of all members. Groups can also be used when creating *access policies* instead of creating a policy for each individual user.

### Roles

A role is a predefined set of privileges in a functional area. PAM has many predefined roles that satisfy most requirements. You can also create custom roles using built-in granular privileges. *Standard user* is the common role that is assigned to general users accessing devices. For a complete list of user roles, see [User Roles](#).

### User Configuration Methods

You can create local user accounts manually or you can import them from CSV files. Users can also be imported from and synchronized with an LDAP user store such as Active Directory. When configured for RADIUS or PKI, users are added when they *first login* to PAM.


### NOTE

Most PAM production deployments use LDAP or RADIUS for authentication.

## Policies

A policy is a set of permissions that is granted to a PAM user or user group to access the interface of a PAM device or device group. For connections using the SSH and RDP access methods, you can even configure [transparent \(automated\) login](#). Simply put, a policy defines the relationship between a *user* and a *device* and results in an access link or links appearing on the Access page of that user.

For example, the following screenshot shows the Access page for a user for whom a policy assigns the SSH Access Method to a device named UNIX-AUX.

Access				
Column:	<input type="text"/>	Value:	<input type="text"/>	<input type="button" value="FILTER"/>
Device Name ▲	Address	Operatin	Access Methods	Web Por
UNIX-AUX	192.168.0.11	Other		

A policy also optionally specifies whether to record all or some of the actions a user performs while accessing a device. Recording can be enabled based on the specified Access Type. *Command line* and *bi-directional* apply to SSH/Telnet and Mainframe sessions. Graphical recording is available for RDP connection and web portal types.

You can create policies manually or can import them from a CSV file.

#### NOTE

Use [Credential Manager](#) to configure Policies with automated login.

#### NOTE

#### More Information

To configure policies to provision user access to devices and applications, do the following procedures in the order shown:

1. [Configure Devices](#)
2. [Configure Users](#)
3. [Provision Access Policies](#)

## Configure Devices

A *device* is a PAM-managed, IP-addressable network node that is the potential access or password target of a PAM user. Devices are displayed, defined, and otherwise managed through the **Devices** menu on the UI menu bar.

#### NOTE

A device that serves a PAM system is not necessarily an access target in that system. For example, a RADIUS authentication server or syslog storage that provides resources to PAM – but is managed by external administrators – is not listed or managed as a device. However, the attributes of that device are specified in the appliance configuration settings.

#### Next Steps



- [About Devices](#)
- [Device Features](#)
- [Device Discovery](#)
- [Device Setup](#)
- [Device Group Setup](#)
- [Device and Device Group Management](#)
- [Device Viewing](#)
- [Set Up Access to a Target Device](#)
- [Socket Filter Agent Support](#)
- [Set up Command Filters](#)
- [Setting Up Transparent Login](#)
- [Set Up the AWS API Proxy](#)
- [Configure Support for Citrix XenApp Resources](#)

## About Devices

A device represents a PAM-managed, IP-addressable network node. A device is a potential target for access or password management by a PAM user. For A2A deployments, a device can be considered a request server. Devices are displayed and managed through the Devices menu on the Administration menu in the UI.

You do configure other devices in PAM that are not Access or Password Management target systems. For example, RADIUS authentication servers and syslog servers provide resources to PAM, but they are not access targets. These systems are not listed or managed from the Devices page in the UI. These servers are typically configured as third-party systems.

### Access to Devices

Privileged Access Manager enables secure access to devices. PAM does not allow connection to any device until it has been approved at the device level. To complete this approval, access methods must be selected. This procedure can be done either when initially creating the device, finishing edits before access is enabled, or to change methods for existing devices.

### Access Types

#### **Software: Access Methods**

The first way that PAM provides controlled access is to specify fully the communication software that is used to implement a connection. The appliance downloads communication executables (implemented as Java applets) from the appliance to the user workstation or other local computer that wraps the user communication within Privileged Access Manager-controlled communication channels.

One applet is defined as the primary communication applet that is named the UP (Universal Ports). The UP is customized by the policy for each *user*, and is always downloaded at each User login session. Meanwhile, the user can download other applets to communicate with the UP to set up and maintain controlled communication to a *device* through Privileged Access Manager. These applets also have custom features, such as command filtering capability. When the session is finished, the applet disappears. These applets are known as **Access Methods**.

#### **Controlled Local Software: Services**

Another approach is to use ordinary (third party) communication software users have on their computers. This software might already be installed, or Privileged Access Manager can supply it (temporarily). Using parameters that are configured by the PAM administrator, the product directs that software to communicate with the UP so that, like an Access Method, a controlled session can be implemented. These definitions are known as Privileged Access Manager **Services**.

An administration user on known ports and to specific applications can create services. These services can include: fat client access such as SQL query front-ends, mainframe clients, and any proprietary applications, which use TCP or UDP connections. The appliance has several ways to do this:

- Download Privileged Access Manager packaged third-party software, such as a commercial SFTP/FTP package.
- Use a local software installation; for example, PuTTY can be available to implement SSH.
- Use Microsoft Windows RDP if the local computer is a Windows device.
- Establish a console.
- Access a web portal using the local default browser.

### ***Restrict Access to a Windows Application: RDP Applications***

Configure RDP applications With Microsoft Remote Desktop Services (RDS), single target hosted applications can be published through RDP instead of allowing access to the entire target device desktop.

### **Terminal Configuration for Device Access**

For line-mode communication, you have a range of options to package the interface. These options can be imposed generally, and then specifically for each Device Group or individual Device.

#### ***Device Types***

Terminal configuration supports the following device types, each with separate functionality and licensing:

- Access Devices
- Password Management Devices
- A2A Devices

#### ***Grouping Devices***

To provision and manage multiple devices, you can use the following two mechanisms:

- **Device Groups** – A set of devices that inherit the same attributes from the group.
- **Tags** – Tags are device attributes that allow you to assign labels to any particular device, and share the labels across many devices. You can filter on the labels to identify sets of devices.

## **Device Features**

### **Device Types**

Devices are categorized into three types. A Device object can represent any physical device logically using one or more of these types:

**Device Licenses** (Licensing page):

- **Access Device:** Network-addressable computing Device (identified by the label "Access" in Global Settings and in a Device template)
- **Password Device:** Device for which passwords are managed (pushed from Privileged Access Manager) are identified by the label "Password Management" in Global Settings and in a Device template.
- **A2A Device:** Device running application clients that connect to Privileged Access Manager to retrieve passwords (identified by the label "A2A" in Global Settings and in a Device template).

A Device Type license permits a maximum number of Devices for each Device Type. The maximum number and the current count of each Device Type appear on the on the Dashboard Overview Tab under License Usage. The same numbers also appear on the System Information dialog.

**License Usage** (Dashboard Overview Tab):

- **Session Management** license: for an Access Device (can co-exist with Credential Manager Device)
- **Credential Manager** license: for a Credential Manager Device (can co-exist with Access Device)
- **A2A Management** license: for an A2A Device

## **Access Types**

Privileged Access Manager enables secure access to devices, and does not allow connection to any device until it has been approved at the device level. To complete this approval, access methods must be selected. This choice can be made when creating or updating the device, or when changing methods for existing devices.

- **Prepackaged:** Standard access methods have been built as **Access Method applets** and do not require any additional software to be installed on a user desktop.
- **Custom:** In addition to the default applet access, virtually any connection application can be configured to allow access by configuring local Privileged Access Manager **Services**.

## **Access Methods**

Several prepackaged Access Method applets are available, with support for VNC, TELNET, SSH, RDP, and serial connections. Default ports can be modified if the application is running on a different port from the one indicated.

Configuration is required at the following levels:

- **Global-level:** For an access method to be available, it must first be permitted (or "switched on") through the Global Settings interface.
- **Device-level:** In addition to the default applet access, Privileged Access Manager can be configured to allow access to virtually any connection application.

## **Graphical and CLI Applets**

- **VNC:** VNC (Virtual Networking Computing) is a graphical desktop remote access application that transmits keyboard and mouse movements. VNC applet access requires a VNC server to be running on the destination device. To use recording, the VNC server must be set in basic unencrypted mode.
- **Telnet:** Administrators often use this tool to connect to UNIX hosts running the TELNET daemon.
- **SSH:** Secure Shell protocol. The SSH applet connects to servers running the SSH daemon. It does not require the client end user to have SSH client software such as Putty loaded.
- **RDP:** RDP is an access method for connecting to Microsoft Terminal Services and is commonly used for administration of Windows servers. The RDP applet is optimized to take advantage of RDP 6.x compression types, with noticeable reductions in file size in comparison with RDP 5.2.

RDP remote device usernames are not prepopulated from Privileged Access Manager login usernames. Instead, the User can populate this name through a field on the [User Information](#) page

### **WARNING**

Due to limitations in XRDP compression support, RDP-to-XRDP sessions use more bandwidth. Session recordings can be much larger than recordings for RDP-to-RDP sessions. Encryption support requires a setting in the xrdp.ini file on the XRDP host.

- **TLS levels:** As of release 2.6, the RDP client (the applet) supports TLS 1.2 connections and supports the TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 cipher suite.
- **Performance:** Sometimes, it is not possible to write an RDP recording to storage as fast as it is being created. In such cases, Privileged Access Manager throttles interaction. From the User point of view, it "slows down." The overall data transfer rate is reduced and writing to the share can be completed.
- **XRDP:** The Privileged Access Manager RDP client applet can also be used to connect with an XRDP server running on a managed Linux Device.

## **Mainframe Applets**

TN3270 and TN5250 are Telnet clients for the IBM mainframe or AS/400 server that emulate 3270 and 5250 terminals and printers. SSL versions are available to provide SSL/TLS support. Support for AS/400-class applet Display Names (TN5250 and TN5250SSL only) is provided on the [User Information](#) page with the Mainframe Display Name field.

- **TN3270**: IBM 3270 Telnet class
- **TN3270SSL**: IBM 3270 Telnet class with SSL
- **TN5250**: IBM 5250 Telnet class
- **TN5250SSL**: IBM 5250 Telnet class with SSL

Due to the variety of target mainframe applications, we do not have a standard automatic login option for the mainframe applets. For TN3270 and TN3270SSL, we offer built-in macros for the username (Ctrl-U) and password (Ctrl-P). During login, the user enters these key combinations to enter the configured user name and password. The password macro only works when the password entry field is hidden, so the password is not visible to the user.

## Services

Services are a way to customize access to the devices. An administrator can create services on known ports and to specific applications. These services can include: fat client access such as SQL query front ends, mainframe clients, or any proprietary applications, which use TCP or UDP connections.

### Prepackaged Services

Services that are prepackaged with the product are identified here.

#### WARNING

Privileged Access Manager ships with several preconfigured SFTP/FTP Services. These services currently support several SFTP/FTP servers including OpenSSH-derived Linux, AIX, and Solaris SFTP implementations. Microsoft IIS SFTP/FTP implementations are also supported with a known limitation when multiple hard drives are present.

While other FTP servers might be compatible, Privileged Access Manager does not test or verify them. The preconfigured services must be used to track target device SFTP/FTP activity to meet compliance requirements for many customers. The activity is tracked in session logs. The service names that are suffixed with "emb" provide the WinSCP client to users without any FTP client application installed. We encourage input on any FTP servers that appear incompatible with Privileged Access Manager, and consider adding support for more FTP servers as business needs permit. Our goal is to provide the most comprehensive access solution for our customers while balancing the need for Access Control and Audit.

## Types

- **sftpftp**: With use of an SFTP client, transports files to and from FTP servers.
- **sftpsftp**: With use of an SFTP client, transports files to and from SFTP servers.
- **sftpftpemb**: This service downloads an WinSCP client to the user desktop. WinSCP is a free and open source SFTP and FTP client for Microsoft Windows.
- **sftpsftpemb**: This service downloads the WinSCP client to the user desktop.

#### WARNING

When running SFTPFTPemb or SFTPSFTPemb, a default option for WinSCP file transfer causes the resulting file to be partially saved. Change the setting for **Preferences, Other general options: Preferences, Transfer: Endurance, Enable transfer resume/transfer to temporary filename for**. Change the default setting of "Files above: 100KB" to "Disable", then users can successfully "PUT" files onto the remote server.

## RDP Applications

With Microsoft Terminal Services, single target-hosted applications can be published through RDP instead of allowing access to the entire desktop. This functionality is only available to servers running Microsoft Terminal Server. On Windows Server 2008, more setup is required.

## Discover Devices on Your Network

To quickly discover and add multiple devices instead of adding each manually, use the device discovery feature, which identifies and registers devices in bulk.

To use device discovery to find network devices and bring them under management by PAM, navigate to **Devices, Discovery** and perform the following procedures:

1. [Create a device scan profile and optionally configure the scan to run on a schedule.](#)
2. [Run a device scan profile manually](#)
3. [View device scan results](#)
4. [Configure PAM to manage discovered devices](#)

Related procedures:

- [Export device information to a CSV file](#)
- [Update discovered devices](#)
- [Delete scan profiles](#)

### Create a Device Scan Profile

Create a device scan profile to specify the properties of the devices that the scan should include or exclude, such as operating systems and IP address ranges. You can also configure the scan to run automatically by configuring a schedule.

1. Select the **Device Scan Profiles** tab and select the **Add** button.
2. On the **Profile** tab, name the profile, and enter an optional description.
3. Optionally, set the **Auto-manage devices** option to automatically put all discovered devices under PAM management.

#### **TIP**

The **Auto-manage devices** option is not set by default because device discovery may identify many devices on your network that you will not want to manage with PAM. If you have a large amount of devices on your network that you will not want to manage with PAM, we recommend that you do not set this option and [manually configure PAM to manage appropriate devices](#) later.

4. In the **Default OS** field, select an OS to narrow the specific discovery criteria or select **Other**.

#### **NOTE**

Device discovery may not reliably identify certain Windows OS versions. If the scan results show an incorrect operating system version, you can change it once the device is under management by PAM. To update the OS, select **Devices, Manage Devices**, and update the **Operating System** field.

5. To specify the number of days after which discovered devices are deleted, set the **Purge Interval (in days)** field. Unless the device is discovered by a different scan profile, the device is deleted. (The default value for the purge interval default is set under **Global Settings, Basic Settings, Scan Purge Interval**.)
6. If device discovery does not determine a location automatically, specify it in the **Default Location** field.
7. Identify at least one target IP address or one device name to include in the discovery on the **Inclusions** tab. You can include multiple entries for each type of target. Select the plus sign to add entries.
  - Specify IPv4 addresses using slash notation (for example, 192.168.2.0/24). All subordinate addresses are included as part of the scan unless there is a corresponding Exclusion address. Wildcards and address range notation is allowed for IPv4 addresses. Use asterisks as wildcards in the format 192.169.0.\*. Specify ranges in the format x.x.x.x-x.
  - If IPv6 is enabled, IPv6 addresses can also be scanned. For IPv6, use CIDR notation (for example, fd6d:8d64:af0c:1:0:242:22:11/120).

**NOTE**

Take care when selecting the CIDR range, as the CIDR value determines the total number of addresses scanned by Device Discovery.

For example, entering `fd6d:8d64:af0c:1:0:242:22:11/120` specifies scanning 256 device addresses, while `fd6d:8d64:af0c:1:0:242:22:11/116` specifies scanning 4,096 device addresses.

- Device name discovery requires configuration of a DNS server in the appliance. Add DNS Servers in the Network Configuration section accessible from the **Config** menu.
8. Optionally, configure the following other settings to refine your scan results:
    - Specify IP addresses to exclude from the scan results on the **Exclusions** tab. Use the same notation as for inclusions.
    - Specify which of the default access methods (as defined on the **Settings, Access Methods** panel), to include in the scan results on the **Access Methods** tab.
    - Specify which services to include in the scan results from those listed on the **Services** tab. The available services are those defined on the **Services, Manage TCP/UDP Services** and **Services, Manage RDP Applications** panels.
    - Specify which device groups (as defined on the **Devices, Manage Groups** panel), to include in the scan results on the **Device Groups** tab.
    - Specify tags to add to discovered devices on the **Tags** tab. Tags are free-form labels that can be added to individual device definitions but which PAM compiles into a list which is available for addition to all devices. You can also create new tags in the **Tag Name** section below the selection columns.
    - Specify available target applications such as SSH, LDAP, and MSSQL to include in the scan results on the **Target Applications** tab.
  9. Optionally, configure a schedule on which to automatically run the device scan on the **Schedule** tab. After you select a frequency, other fields appear. Select the appropriate time intervals.
  10. Select **OK** to save the scan profile.

**Run a Device Scan Profile Manually**

To run a device scan manually, select the scan profile from the **Device Scan Profiles** list, and select the **Run** button.

**NOTE**

You can also create a schedule to run a scan when configuring the [device scan profile](#).

**Review the Status and Results of Your Device Discovery Jobs**

The topics in this section describe how to use the various ways you can view the status and results of your device discovery jobs.

***View the Status of Discovery Jobs in Progress***

Once a scan is running, review its progress on the **Discovery Jobs** tab. You can also cancel the job on this panel by selecting the **Cancel Job** button. Once it is complete, view a summary of its results on the **Device Scan History** tab.

**NOTE**

The **Discovery Jobs** and other tables are refreshed according to the **Table Refresh Interval** value set on the **Basic Settings** tab on the **Global Settings** panel. The default value is 60 seconds.

***View the Results of Completed Device Discovery Scans***

This content describes how to use a number of ways to view different information about the results of device discovery scans.

Navigate to **Devices, Discovery** and select the **Device Scan History** tab to open the **Most Recent Scans** panel from where you can access the results of all completed device discovery scans. The panel provides a sortable, filterable table

of the most recent scans, each row showing the name of the scan profile, when it was last run, and summary values for the following details:

- **Devices:** The total number of devices discovered.
- **New:** The number of new devices discovered since the scan profile was last run.
- **Not Found:** The number of devices that were discovered the last time the scan profile was run but *not* found by the latest scan.

#### NOTE

Select any of the summary values to open the **Scan Results** dialog at the corresponding tab. That is, selecting the **New** value displays the **New Devices** tab.

To see different views of a device scan on the **Most Recent Scans** panel, select the corresponding table entry and select one of the following buttons:

- **View Summary Details:** Opens the **Scan Results** dialog at the default **Scan Information** tab, which displays the scan profile name and the job time. The **Discovered Devices**, **New Devices**, and **Not Found Devices** tabs list the names of the corresponding devices. The **Logs** tab displays a table including each action that is taken regarding this scan.
- **View Scan Results:** Displays a table of the following information about discovered devices: device name, operating system, and status. The checkboxes in the "Is Managed" column specify whether devices are currently managed by PAM [and allow you to change that state](#).
- **View Scans:** Shows all the scans that are run for a given profile. The resulting table lists details for each job. Select a Scan Discovery Time and either View Summary Details for lists of discovered device names (use **View Scan Results** for detailed, updatable information).

To see all discovered devices rather than only devices for a given scan, select the **Discovered Devices** tab at the top of the Discovery panel.

#### NOTE

The number of items in the **Device Scan Results** is controlled by the **Global Settings** panel. **Default Screen Size**, under Basic Settings, defaults to 30. This option also controls the number of items that are shown in the Device discovery lists.

### View the Details of All Discovered Devices

To view the details of all discovered devices, navigate to **Devices**, **Discovery** and select the **Discovered Devices** tab, which displays a list of all discovered devices, their operating system, scan status, and latest discovery time. The checkboxes in the "Is Managed" column specify whether devices are currently managed by PAM [and allow you to change that state](#).

### Manually Configure PAM to Manage Discovered Devices

By default, the **Auto-manage devices** option in the device discovery profile is not set so the discovery job does *not* automatically place discovered devices under management by PAM. This is because device discovery may identify many devices on your network that you will not want to manage with PAM. This also allows you to "stage" devices and verify that they are valid before configuring PAM to manage them.

To enable access control and credential management for discovered devices, configure PAM to manage those devices.

**To configure PAM to manage specific discovered devices, follow these steps:**

1. Open the panel that displays the devices that you want to bring under PAM management:
  - Navigate to **Devices**, **Discovery**, select the appropriate scan profile entry, and select the **View Scan Results** button.
  - Navigate to **Devices**, **Discovery** and select the **Discovered Devices** tab
2. Select the rows of the devices that you want to manage.
3. Select the **Manage** button above the "Is Managed" column and select **Yes** in the dialog that appears.



To configure PAM to manage *all* discovered devices, follow these steps:

1. Navigate to **Devices, Discovery** and select the **Discovered Devices** tab
2. Select the **Manage All** button.

### **Export Devices**

Select the **Export** button to send detailed information about each discovered device to a CSV file.

### **Update Discovered Devices**

Select the **Update** button (which is only active for one device selection at a time) to display the **Update Discovered Device** dialog. The various tabs allow you to change the management, access methods, services, and applications associated with the selected device. The **Device Information** tab provides details, such as IP address, OS detail, status, and other information.

#### **NOTE**

The number of items in the **Discovered Devices** list is controlled by the **Default screen Size** setting on the **Basic Settings** tab of the **Global Settings** panel and defaults to 30. This setting also controls the number of items that are shown in the **Device Discovery** lists.

### **Delete a Device Scan Profile**

To delete a profile, select the scan and select **Delete**. The scan is deleted from the Device Scan History. The appliance also deletes any devices that are associated with that profile, unless the devices are associated with another scan profile.

## **Device Setup**

This topic describes how to use the **Manage Devices** screen to add devices.

### **Prerequisites for Adding a Device**

If necessary, set up access types before device setup. These types include:

- **Access Methods** invoke a proprietary Java applet that is downloaded from Privileged Access Manager to a local client computer. See [Access Methods](#) for more information.
- **TCP/UDP Services**: See [Create TCP/UDP Services](#) for more information.
- **Native Services** invoke a resident application on a local Client computer.
- **Web Portals** invoke an HTTP/HTTPS website. See [Configure Automatic Login to Web Portals](#) for more information.
- **RDP Applications** invoke resident application on target RDP Device. See [RDP Applications Configuration](#) for more information.

### **Basic Info Configuration**

The following procedure describes how to configure basic information for your device.

**Follow these steps:**

1. Log in to the UI.
2. Select **Devices, Manage Devices**.
3. To specify a new device, select **Add**.
4. Complete the fields on the **Basic Info** tab. Required fields are highlighted with a red asterisk.
  - **Address**: The device IP address or FQDN.

#### **NOTE**

Any literal IPv6 address entered in the **Address** field will be normalized according to the following standard: [RFC 5952: A Recommendation for IPv6 Address Text Representation](#).



For example, entering 1111:2222:000A:000B:0:0:0:D in the **Address** field, and then saving it, means this value converts to 1111:2222:a:b::d, enforcing the lowercased and compressed value according to the RFC 5952 standard.

- **Name:** This field specifies the name that is displayed on the Access page. You can enter double-byte characters.
- For FQDN, DNS must be set up properly on the **Configuration, Network, Network Settings** page.
- A specified FQDN can be no longer than 255 characters.
- If you are updating a Device that is imported from AWS, Azure, or VMware, an **Override Address** checkbox appears. To edit the Address, for example, to use a private IP address, select the Override Address checkbox.

**Scan:** Select this option to execute a port scan. The scan detects services that are configured. The detected services appear on the Access Methods and Services tabs. **Description:** Enter an optional description. **Location:** Enter an optional location. To help you organize your device list, you can sort entries in this column. **Operating System:** Select the device operating system from the drop-down menu. To help you organize your device list, you can sort entries in this column.

#### NOTE

If you are adding a device for a PAM SC Utility Appliance, select **Utility Appliance** from the drop-down menu. For more information, see [Configure PAM Devices for Utility Appliances](#).

**Version:** The **Version** field only appears for PAM SC devices.

#### NOTE

The **Version** field does not appear for non-PAM SC devices.

**Device Type:** Select the functions that you want to apply to the device:

- **Access** for access to remote systems
- **Password Management** for designating a device as a target device for credential management.
- **A2A** for Application-to-Application credential management. An A2A Client must be installed on the remote system: The following other A2A fields are required:
  - **Active:** Select **Active** to allow the A2A Client to receive credentials
  - **Preserve Hostname:** Select this box to prevent the host name of the request server from being overwritten each time the A2A Client registers. If you do not select this option, the existing host name can be overwritten.

5. Select **OK**.

## Tag Creation and Assignment

Device tags are text strings of any form and length that you can use to group and search for Devices. Tags have no dependence on any other characteristics of those devices. You create a device tag within a specific device record. After it is created, you can copy the tag to other devices. Multiple tags can be assigned to a device, so it is possible to create a wide variety of groupings.

A tag is applied to a device record. How you apply a tag depends on whether it exists or you are creating a tag:

- For an existing tag, select from drop-down list of tags. An existing tag must be used in at least one device record. Start typing and a list of available tags appears in the drop-down list.
- For a new tag, enter a tagname.

To view and edit tags, see [Manage Tags](#).

The following guidelines apply when you tag devices and device groups:

- A device in a device group does not inherit the tag that is assigned to the device group.
- If a device and a device group have the same tag, PAM treats the single device as part of the device group. If a single device has the same tag as a device group, any policy that applies to the device group also applies to the device.

**Example of Using Tags:** A number of devices use the Windows operating system, but some do not. For network maintenance purposes, you want to group all Windows devices. Tag all devices with the tag **Windows**. On the Manage Devices and Access pages, you can then search for "windows" to collect all instances.

## **Specify Access Methods**

From the **Access Method** tab, specify the method by which users gain access to a device. The default methods are RDP, SSH, Telnet, and VNC. Mainframe licenses also provide the following methods: TN3270, TN3270SSL, TN5250, TN5250SSL

### **Follow these steps:**

1. Select the **Access Methods** option.
2. Select the plus sign to add a method.
3. In the **Name** field, select an access method from the pull-down menu. The **SSH** access method can provide X11 forwarding using SSH. To enable X11 forwarding, select the **X11** checkbox. For forwarding to work, the client computer must have a configured X11 server, such as OpenText Exceed. Be aware of the following limitations with X11:
  - The product supports key stroke logging and command filtering for all activities that are conducted within the SSH applet. However, the X11 server runs on the local client, so it cannot provide graphical session recording or command filtering for the forwarded graphical application.
  - The X11 feature cannot currently be applied to device groups.**RDP** has a **Console** checkbox to specify that access is through the device console interface.
4. Optionally, specify a **Custom Name**. The default Name is the Access Method (such as SSH). A custom name is required if a device uses the same access method on two different ports. For example, if a device listens for SSH connections on port 22 and on port 2200, you define an SSH access method for each port. Both access methods cannot have the same name, so at least one of them has to have a custom name. You can also use a custom name to have a non-standard name appear on the access page for this method on this device.
5. In The **Port** field, accept the default port or specify a different port number.
6. Repeat the previous steps for each method you want added.
7. Select **OK** to save your selections, or continue to the next tab.

## **Select Services**

Select services to customize access to devices.

### **Follow these steps:**

1. Select the **Services** option.
2. For each service you want, select the associated checkbox.
3. Select the right arrow to move the services over to the **Selected Services** list.
4. Select **OK** to save your selections, or continue to the next tab.

### **NOTE**

If this target device will be used by a PAM Agent, verify that the **IP Version** setting of any selected service matches the type of IP address (IPv4 or IPv6) specified in the **Address** field on the **Basic Info** tab. For more information, see [Create TCP/UDP Services to Access a Device](#).

## **Customize Terminal Access to a Device**

Set up terminal access to a device so that any user receives an administrator-recommended screen presentation. Configuring the look of the terminal is helpful for users who do not know the ideal settings.

A user can override this customization by specifying user-based terminal settings.

### **Follow these steps:**

1. Select the **Terminal** option.
2. Configure each field using the pull-down lists. Most fields are self-explanatory.

**NOTE**

The "End to select" checkbox function is deprecated.

**Transparent Login**

Transparent login lets a user issue password-enforced commands whose passwords are unknown to the user. The user must be logged on to a target device to use transparent login.

The RDP and SSH services support transparent login. Support for the graphical RDP transparent login feature on Windows machines is on the [Services](#) page. Support for the SSH applet and the SSH proxy is also defined on the Services page. Specify one or both UNIX/Linux applications **pbrun** or **sudo**. When these applications are invoked, the applications are silently presented with valid managed credentials, effecting an automated transparent login.

To use sudo/pbrun at run time, specify a credential for auto-connection on the policy for this device, and select the Transparent Login checkbox.

**Follow these steps:**

1. Select the Transparent Login tab.
2. In the drop-down list, select sudo/pbrun. The **sudo/pbrun** fields appear.
3. In the **Full Path** field, enter the path on the target device where the application executable resides. For example, /usr/bin
4. In the **Password Prompt** field, specify a substring of the text that is presented to the user. The closer a string match that you provide, the greater the security. For example, the full prompt to the user might be **sudo password** for *user*, where *user* represents the dynamically applied user name. The maximum literal that can be applied is then "sudo password for".

**Command Strings for Transparent Login**

You can also specify a set of command strings and a prompt. This feature is disabled by default for security reasons. To enable it, go to **Configuration, Security, Access**, and select **Enabled** for **Command String**.

**To use the Command String feature, follow these steps:**

1. Enable **Command String** on the **Configuration, Security, Access** page.
2. Select the Transparent Login tab.
3. In the drop-down list, select **Command String**. The **Command String** fields appear.
4. In the **Authentication Prompt** field, specify a substring of the text that is presented to the user. The closer a string match that you provide, the greater the security. For example, the full prompt to the user might be password for *user*, where *user* represents the dynamically applied user name. The maximum literal that can be applied is then "password for".
5. Select the plus icon to add the actual command string. The user must match the command string exactly. To support shortened versions of the command string, add them as separate command strings. For example, "ENABLE" would be one command string, and "EN" would be another command string.
6. Select **OK** to save your settings.
7. [Set Up a Policy](#) for the device and an account to use the transparent login feature. Unlike sudo/pbrun, auto-connect configuration is unnecessary for Command String transparent login. The password from the specified target account is sent under the following conditions:
  - You type a string that matches the specified command string.
  - SSH returns the specified prompt, whether you are using an SSH applet or the SSH proxy.

## Check PAM SC Server Control Policies

The **Server Control** tab appears for all PAM SC devices except the following devices:

apikey.xceedium.com	tap.ca.com
ca.portal.azure.com	Utility-Server
nim.pam.ca.com	xceedium.aws.amazon.com
server.control.policies.pam	xceedium.nsx.vmware.com

The **Server Control** tab has two sections:

- **Policies Assigned:** Contains the list of policies assigned on the device.
- **Policies Deployed:** Contains the list of policies deployed on the device.

When assigning a server control policy on the server control device, it takes some time for the server control device to get this deployment information. All the assigned (queued) policies appear in the assigned table. Once the server control receives this deployment information, the policies appear the **Policies Deployed** list.

### Follow these steps:

1. To view the policy deployment status of the device agents, navigate to **Devices, Manage Devices**.
2. Select a device, and then select **Update**.
3. Select the **Server Control** tab.

## Check the Status of Agents

Use the following steps to check the status interval for Agents (endpoint devices) using PAM Integrated Server Control.

### Follow these steps:

1. To view the status of the device agents, navigate to **Devices, Manage Devices**. A list of Server Control, UNAB, and PUPM devices appears.
2. Select a device, and then select **Update**.
3. Select the **Agent Status** tab.
4. The **Agent** type, **Version**, **Activation Date**, **Last Update** for policy, and the **Utility Appliance** address appears.
5. Select **OK** or **Cancel** to exit this screen.

## Add a UNAB Configuration Token to a Device

Do this procedure to add a UNAB Configuration Token to a device. **Follow these steps:**

1. In the PAM UI, select **Devices, Manage Devices**.  
A list of all devices appears.
2. Select the UNAB device, and then select **Update**.  
The **Update Device** page appears.
3. Select the **UNAB** tab. The current **UNAB Configuration Token Update** page appears.
4. Select the **+** icon. A new blank row appears.
5. Select the appropriate section, token, and value from the drop-down menu.
6. Select **OK**.

## Edit a Device from a Policy

An administrator can edit a Device from the Manage Policies page.

1. Open the **Policy, Manage Policies** page.

2. Select a Policy to **Update** for a given Device.
3. Select the **Manage Device** button on the Policy window. The corresponding **Device** window appears.

### **Edit Targets from the Manage Devices panel**

An administrator can add a Target Application from the Manage Devices page:

1. Select a Device from the list, then select the **Manage Target Applications** button. If the Device record is already open, you can select **Save and Add Target Applications** at the bottom of the Device window.
2. The Add Target Application window opens in front of the **Target Applications** List. The GUI controls are presented as they are on Targets, Target Applications.
3. When finished, select **OK**.

#### **NOTE**

For information about importing Devices using a CSV file, and importing AWS and VMware Devices, see [Import and Export Devices](#).

## **Import and Export Devices**

As a Privileged Access Manager Administrator, you can import a device list in CSV format as an alternative to adding the devices individually. You can also export Devices and Device Groups. You can import AWS and VMware Devices, and Azure VMs.

### **Use a CSV to Import Devices and Device Groups**

You can import a CSV file with a list of Devices. A sample file can be downloaded by selecting **Devices, Manage Devices, Import/Export**, and **Download Sample File**. The sample file lists all of the required fields. You can use the format to manipulate an existing device list from another source, such as an inventory control database. For detailed information about the columns in the CSV file, see [Device Groups and Devices](#).

#### **NOTE**

Do not import a CSV of Devices and Device Groups that are provisioned by LDAP, AWS, VMware, or Azure. These types are ignored on import and should be managed according to their specific procedures, found on this page.

### ***Configure Internet Explorer***

To use the Import/Export functions with Internet Explorer (IE), changes might need to be made to the security settings. To establish IE security settings:

1. Open IE browser.
2. Select **Tools, Internet Options**.
3. In the Internet Options pop-up window, select the **Security** tab.
4. Select the slider zone
5. Select **Custom level**. Scroll to **Downloads**. For **File download**, select the **Enable** option.
6. Select **OK** to save changes.

### ***Import Devices from a CSV***

To import the Devices, follow these steps:

1. Go to **Devices, Manage Devices**.
2. Select the **Import/Export** button.  
The Import/Export Devices window appears .
3. Select Download Sample File, and save the file.

4. Create a CSV file from the downloaded template.

#### CSV Format

- Do not change the heading (first) row text.
  - New Device records:
    - Not all fields are required. Required fields include: **Type**, **DeviceName**, **Address**
    - For any fields not used: Preserve all headings on the first row, but leave other row cells blank.
  - Updates to existing Device records:
    - Each Device Group is represented by a line record with Type="device group".
    - Device Group records should be at the top of the file, ahead of all Device records.
    - Device membership in a Device Group is indicated in the Group Membership column.
5. In the **Import/Export Devices** window, select **Choose File** to select the file, and select **Import Devices**. The content of the file is added to the existing Device database. The new content does not replace the current database.
  6. Navigate to **Devices**, **Manage Devices**, and confirm that the import was successful by inspecting the Device list.

#### Use a CSV to Export Devices and Device Groups

A CSV list of all configured devices can be downloaded by selecting **Export Devices**. This exported file can be used to make a revised version, and then imported back into Privileged Access Manager.

#### WARNING

If you export a device file containing Special Type devices, the file does **not** contain the password. If you reimport that file into Privileged Access Manager, the passwords are not present in the import.

#### Import from AWS

After you configure access to an AWS account and activate **Enable Syncing**, the instances in that account with **State** green/"running" are imported as Devices. Instances that are tagged in AWS with the tag key **xsuiteignore** are not imported. The list is refreshed according to the **Configuration, 3rd Party** parameter **Enable Syncing**, or upon clicking the **Refresh AWS Devices** link at the top.

The Device records created cannot be deleted except upon disconnection from AWS.

The following Device attributes are populated from AWS instance attributes, and cannot be edited:

- The AWS **Name** and AWS **Instance** ID are combined to create a Device **Name** of "awsName ( awsInstance )".
- The Device **Operating System** is populated.

The following Device attributes are populated from AWS instance attributes, and *can be* edited in the Device record:

- Access Methods are populated with:
- **RDP** using port **3389** for Windows OS
- **SSH** using port **22** for UNIX and Linux OS

The Device **Address** is populated with the AWS **Public DNS**. To edit the Address, for example to use a private IP address, select the **Override Address** checkbox next to the Address field. The Override Address checkbox only appears for Devices that are imported from AWS, VMware, or Azure.

The device **xceedium.aws.amazon.com** is a Credentials Management placeholder Device. This device is created when AWS is configured to manage AWS access keys in Privileged Access Manager. It cannot be edited, but is created/removed in synch with an AWS configuration **Save**.

## Import from VMware

After Privileged Access Manager is configured in **Configuration, 3rd Party** to access a VMware account and **Enable Syncing** is activated, the instances in that account import as Devices. Instances that have been tagged in the VMware appliance **Summary, Annotations, Notes** field with the string: **Xsuitelgnore** (anywhere in the field) are not imported.

The list is cyclically refreshed according to the **Configuration, 3rd Party** parameter **Enable Syncing**, or upon clicking the **Refresh VMware Devices** link.

- During import, each virtual machine (instance) in VMware results in the creation of a Device
  - The Name of the Device that is created is the combination: "VMwareInstanceName – vm- nn" where "nn" is a VMware assigned number.
  - When available, the internal Address of each Device is provided; otherwise it is marked as "Not-Active- VMwareDeviceName - vm nn".
  - To edit the **Address**, for example to use a private IP address, select the **Override Address** checkbox next to the Address field. The Override Address checkbox only appears for Devices that are imported from VMware, AWS, or Azure.
- During import, each folder in VMware results in the creation of a Device Group
  - The Name of the Device Group that is created is the combination: "VMwareFolderName - group-v nn" where "nn" is VMware assigned number. You can edit it.
  - The Group Type is "VMware", and cannot be edited.
  - The Description is "VMware derived group", and can be edited.
- All VMware imported Devices are members of a VMware-determined Device Group. For VMware instances with no containing folder (in VMware), the Device Group named "VM" is used.

## Import from Azure

After you configure an [Azure connection](#) and activate syncing, the instances in that account are imported as Devices. The list is refreshed according to the **Refresh Interval** on the **Configuration, 3rd Party, Azure** page. You can immediately refresh them by selecting the **Refresh Azure Devices** link at the top of the **Manage Devices** page.

To prevent specific devices from importing, you can "tag" them in Azure. Follow these steps:

1. In Azure, select the Virtual Machine that you want to prevent importing.
2. Select **Tags** from its menu.
3. Select the **Name** drop-down list. If the **PAMIgnore** tag is not listed, enter `PAMIgnore`, and set the **Value** to `true`.
4. Select **Save**.  
The Tag is applied and available for every device in your Subscription.
5. Repeat for each VM that you want to ignore.
6. To see all tagged VMs, enter "Tags" into the **Search** field.  
The Tags list appears. Select a Tag to see all the objects to which the Tag is applied.

The imported Device records cannot be deleted except upon disconnection from Azure. The following Device attributes are populated from Azure instance attributes, and cannot be edited:

- The Azure Name is the Device Name
- The Location is the Azure location of the instance
- The Device Operating System is Linux

The following Device attributes are populated from Azure instance attributes, and *can be* edited in the Device record:

- Description
- Access Methods are populated with:  
**SSH** using port **22** for UNIX and Linux OS



The Device **Address** is populated with the Azure **Public IP**, or if DNS is set for the device in Azure, the **FQDN**. After you import a Device, you can edit its Address, for example, to use a private IP address. Follow these steps:

1. Select **Devices, Manage Devices**.
2. Select the Device and select **Update**.
3. On the **Basic Info** tab, select the **Override Address** checkbox.
4. Edit the **Address**.
5. Select **OK** to save.

The device **ca.portal.azure.com** is a Credentials Management placeholder Device, which is created when your instance is licensed. This Device manages Azure access keys in Privileged Access Manager. All Azure target accounts should be associated with this device.

### **Import from LDAP**

To import a Device Group from LDAP, see [Import LDAP Device Groups](#).

## **Device Group Setup**

Learn how to create PAM device groups to group devices that share common access methods and functionality.

Though any devices can be a member of a device group, group functionally similar devices. Before you can add a device to a group, you must first configure a device with Password Management as its device type.

When using device groups, the action **deny** takes precedence, unless otherwise specified. The service is available at the group level only if it is available at the device level. The most restrictive policy is used when a conflict arises.

The following topics apply to device groups:

### **Credential Sources for Device Groups**

A *credential source* is a particular target device or set of devices that stores user credentials. An Active Directory Server is an example of a credential source. If you specify a credential source for a device group, PAM can find the credentials that are applicable to devices in that device group. PAM uses these credentials to enable a user to log in to any device in the group.

#### ***Using Multiple Credential Sources***

You can assign more than one credential source for a particular device group. If you configure multiple credential sources, PAM gathers all available credentials from all sources. The appliance then creates a combined list of target accounts for a specific set of users or many users and applications.

A device group does not have to include the credential source device. If you exclude the credential source from the group, you can avoid creating a policy that provides direct access to the credential source. Instead, the group contains only the devices that rely on the credential source for authentication.

Credentials from any target account that is associated with any credential source can be used to access any device group member.

#### ***Using Credential Sources in a Policy***

When you configure a policy for a device group, all accounts from the multiple credential sources are available for selection. When a user initiates a connection, these administrator-selected options are presented so that the user can select one. You can use all access methods and services that are configured for the devices in a device group with one or more credential sources.



## Add or Modify a Device Group

1. On the **Devices, Manage Device Groups** page, select **Add**.  
The **Add Device Group** window opens.
2. Enter a **Name** and **Description** for the group. Double-byte characters are supported.
3. Select the type of group to provision from the **Provision Type** dropdown menu: **(Local)** for all device groups unless you are setting up the group for AWS.
  - **Local** (Default): Provision any type of device group except AWS
  - **AWS**: Provision an AWS device group.

### NOTE

AWS groups are determined by settings on the **Configuration, 3rd Party, AWS** page. AWS device groups act as a container for devices that are created as a result of importing AWS devices. Each device should have a tag Key of "PamGroups " and a Value of "[PAM Group Name]". Following import, the group cannot be deleted unless the AWS configuration is cleared from **Configuration, 3rd Party, AWS** or the group becomes empty. The group is updated according to the schedule in the AWS Configuration.

4. Optionally, select one or more **Credential Sources** from the available device list.
5. Optionally apply tags on the **Tags** tab, if available.
6. On the **Access Methods** and **Services** (to Access Type members) tabs, select Access Methods and Services to enable them for group members.
7. On the **Enable** tab, you can:
  - **Provide Credentials for 'Always Prompt For Password'**: If a Windows device has this setting, you can automatically provide obfuscated credentials. See [Enable a Password Push for RDP Password Enforcement](#) for details.
  - **Handle 'Legal Notice' on Logon Screen**: Select this option to handle the "Legal Notice" during login. This option only works when **Provide Credentials for 'Always Prompt for Password'** is enabled.
8. The **Server Control** tab only appears for PAM SC devices. This tab has two sections:
  - **Policies Assigned**: Contains the list of policies that are assigned on the device.
  - **Policies Deployed**: Contains the list of policies that are deployed on the device.

## Create an AWS Device Group for Linux/UNIX Devices

In AWS, Linux and UNIX instances use AWS Key Pairs. If all instances in a planned Device Group use the same key pair, a group policy can be provisioned to use that key pair for auto-connection.

1. Create an AWS Type Device Group.
2. Assign an AWS instance with imported Devices to it, all of which use the same key pair.
3. Create a policy with that Device Group.
4. From the SSH applet credential pop-up box, select the key pair that is held in common.

This key pair is used for auto-connection for any Device in the group.

## Edit a Device Group from the Manage Policies Page

An administrator can edit a Device Group record by invoking it directly from the Manage Policies page.

### Follow these steps:

1. Open the Policy, Manage Policies page.
2. Populate the Device (Group) field with a record name.
3. Double-click the name to display its editing template in a shadow box window.
4. When finished, select Save (or Cancel) to return to the Manage Policies page.

### NOTE

For information about importing an LDAP Group, see [Import LDAP Device Groups](#).

## Import LDAP Device Groups

An efficient method of creating an LDAP device group is to import an LDAP group from a remote LDAP server. To complete an import, you are required to use the built-in *PAM LDAP Browser*, which gets launched during the import procedure.

This topic explains the following tasks:

Only a Privileged Access Manager administrator has privileges to import an LDAP group.

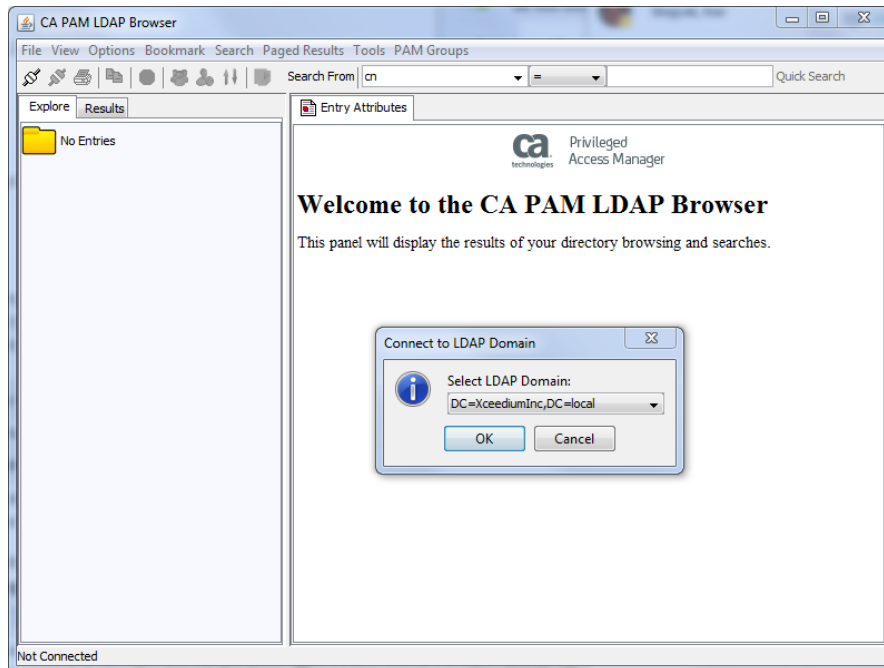
### Launch the LDAP Browser

Use the LDAP Browser to import an LDAP group.

#### Follow these steps:

1. Verify that your appliance is licensed. A license is required to launch the LDAP Browser.
2. Navigate to **Configuration, 3rd Party, LDAP** to configure access to an LDAP server. Provisioning the LDAP server is necessary to make LDAP groups available for import.
3. Select **Devices, Manage Device Groups**.
4. Select **Import LDAP Groups**.

The LDAP Browser launches. You are prompted to select an LDAP domain.



5. Go to the next procedure to import the LDAP group.

If the LDAP server does not support the cipher suite that is used by the Privileged Access Manager LDAP browser, a connection failure occurs. The following error message appears:

“Possible cipher mismatch with LDAP server.”

During provisioning, ensure that the ciphers that are supported on the target LDAP server include those ciphers that are supported by the LDAP browser.

### Cipher Suites Supported by the LDAP Browser

The LDAP browser supports newer cipher suites including Diffie-Hellman cipher suites that enable Perfect Forward Secrecy (PFS) and better performance through the elliptical curve.

- **(Default) When TLSv1.0 and 1.1 are allowed, the following ciphers are available for negotiation with the LDAP/Active Directory server:**

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA  
 TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
 TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA

- **When TLSv1.0 and 1.1 are disabled (only TLSv1.2 is enabled), the following ciphers are available:**

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

#### **NOTE**

When you change the TLS configuration, the current LDAP browser connections are not affected. The configuration changes take effect after the LDAP browser is launched.

- **When FIPS mode is enabled, the following ciphers are available:**

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

When TLS 1.0 and 1.1 are disallowed in the Privileged Access Manager configuration, SHA-1 HMAC is disallowed and only SHA256 is used.

The only Supported Elliptic curves are -secp256r1, secp384r1. These curves are NIST approved. Microsoft Windows can set curve support by group policy to ensure that the Active Directory Server allows Privileged Access Manager curves if ECDHE is required.

### **Import LDAP Groups**

In the LDAP Browser, the **Explore** tab in the left pane shows a graphical representation of an LDAP tree. Select any object to see the object attributes.

#### **Follow these steps:**

1. Select the LDAP domain and select OK to connect to it.  
The browser connects and displays all records below that domain.
2. Navigate the LDAP tree in the left pane and locate the device group that you want to import. Traverse the tree in any order or direction.
3. To import a device group to import, select the checkbox next to the group.

4. Repeat these steps for each group you want to import.
5. (Optional) Review the device groups that are selected for import:
  - a. Select **PAM Groups, Manage selected groups to register with the PAM appliance**.  
The list of the Distinguished Names for all selected groups displays.
  - b. Select and edit any group DN, or remove it from the staging list.
6. Select **PAM Groups, Register selected groups with the PAM appliance**.  
A window opens displaying a list of the staged groups. You can watch the progress, and can display any messages that are associated with the actions.
7. When ready to import the groups, select **Register Groups** in the lower-left corner.  
Privileged Access Manager imports the groups in the order that they are listed. The browser provides feedback and cancellation options throughout the process.

**TIP**

You can cancel registration of a group, or you can cancel the registration of all groups, even after they have started.

When the imports are finished, each line item in the registration window shows a green checkmark for success or a red **X** for import failure/cancellation.

8. (Optional) Review the status of the full list and each individual group by selecting its line item. If you made any changes, or any errors occurred for an individual group, the lower **Messages** panel provides details
9. Go to **Devices, Manage Device Groups**, and confirm that the imported groups appear on the page.

**NOTE**

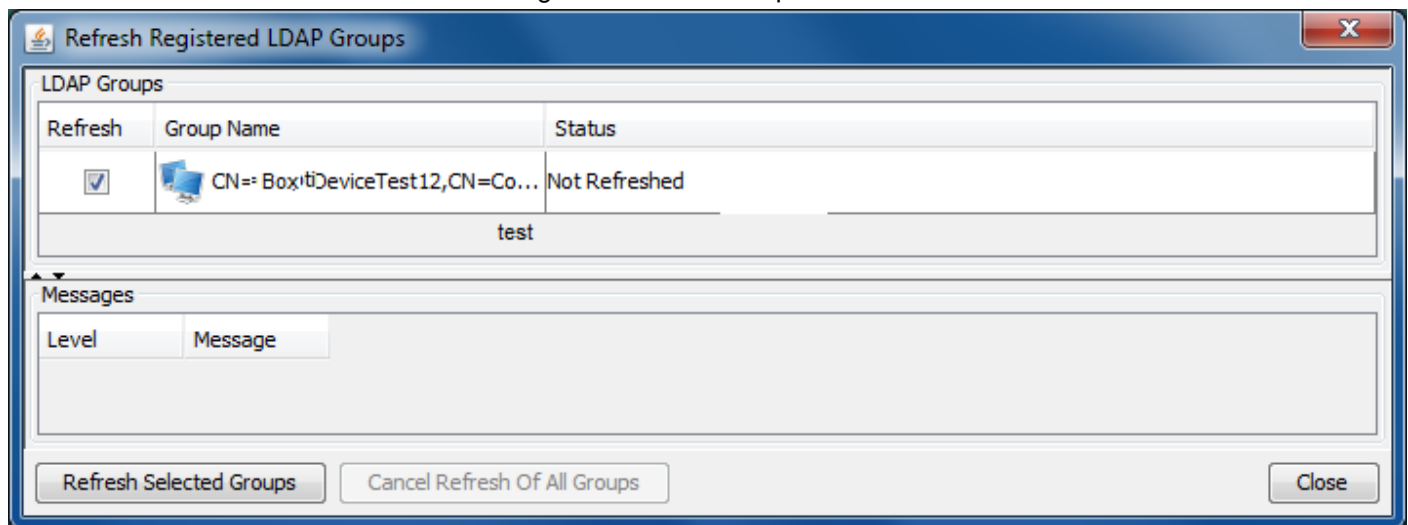
You cannot delete a record from an imported device group. Also, you cannot edit an LDAP-imported field.

**Refresh LDAP Groups**

You can refresh an LDAP Group to update the records in the group.

**Follow these steps:**

1. In the UI, select **Devices, Manage Device Groups**.
2. Toward the right side of the page, select **Refresh LDAP Groups**.  
The LDAP Browser launches the Refresh Registered LDAP Groups window.



3. Select one or more groups you want to refresh and select Refresh Selected Groups.

**Refresh Active Directory Device Groups After an OU Change**

A change to organization unit (OU) of a device results in a change to the device DN. The modified DN can impact an access policy. PAM handles an OU change when the Active Directory group is refreshed automatically. During a refresh, the appliance searches the remote Active Directory Server and updates its device record. Despite the OU change, the policy for that device is preserved.

### **WARNING**

To reflect an OU change immediately, you can manually refresh an Active Directory group in PAM. To keep the data in sync with Active Directory, refresh all the groups that now include the device *and* all the groups from where the device moved.

### **Nested LDAP Groups**

An LDAP group might be nested within another group as an element in a parent group member attribute. When the parent group is imported, all devices in the parent or the child are imported. For example, consider groups StateA and CityB, where group CityB is a member of (nested in) the group StateA. If you import the StateA group, you see every member of StateA and every member of CityB.

### **LDAP Browser Menus and Controls**

The following table shows LDAP Browser controls.

Menu Item	Function
Copy icon	Copy the Distinguished Name of selected entry to the Clipboard.
Group icon	Display all the groups in this container. After selecting an object in the tree under the Explore tab, click this button. You then switch to the Results tab, under which you see a fully expanded tree of all groups (objectClass: group) contained within the selected object.
<b>File</b>	
Connect	Log in to an LDAP database. Invokes a pop-up window from which you can select from currently accessible domains.
Disconnect	Log out from the current LDAP domain.
Print	Print currently selected node.
Exit	Close browser window. <b>Note:</b> The browser continues running while a connection is active. During that time, the browser can be invoked again from the Devices, Manage Device Groups, Import LDAP Group.
<b>View</b>	
Show Button Bar	Below the main menu bar, at the left side Default: On
Show Search Bar	Below the main menu bar, at the right side Default: On
<b>Options</b>	
Set LDAP Connection Timeout	Maximum time (seconds) before a connection attempt is canceled. This timeout is useful when multiple servers are specified for a particular LDAP domain. Default: 60 seconds

Set Result Set Page Size	Maximum number of records in an LDAP directory before pagination is triggered for representation in the browser tree. Number of records in each page of a paginated subtree. Default: 1000
<b>Bookmark</b>	A bookmark can be made on any leaf in a tree so you can select it later from the menu. Bookmarks are saved for each domain, and appear only when the browser is connected to that domain.
Add Bookmark	Opens an editing window for bookmarking currently selected leaf: DN – pre-populated with the current Distinguished Name (DN) Bookmark Name – pre-populated with the current Common Name (CN) Description
Edit Bookmark	Opens a bookmark selection window. Selection in turn opens a bookmark editing window (see Add Bookmark).
Delete Bookmark	Opens a bookmark selection window. Selection in turn deletes and confirms deletion of the bookmark.
<b>Search</b>	
Search Dialog	Opens a detailed search specification window. (Contrast to Quick Search.)
Delete Filter	Opens a window with a list of filters for selection and deletion.
Return Attribute Lists	
<b>Paged Results</b>	
Next Page of Results	Retrieve next page of results and display page wrapper in the Explore tree (when green; otherwise, gray when inapplicable).
<b>Tools</b>	
Stop Action	Suspends an LDAP request. Suspending a request is useful when the page size is large and the browser is searching a large database.
Privileged Access Manager <b>Groups</b>	Privileged Access Manager-specific menu items
Manage selected groups to register with the appliance.	Lists all items that are currently selected (or staged) for import to Privileged Access Manager.
Register selected groups with the appliance	Perform the input operation on the items that are selected, which are listed in Manage selected groups to register with the Privileged Access Manager appliance.

Icons appear in the Button Bar menu when that menu is active (or "on"). By default, the Button Bar is on.

## Device and Device Group Management

The following functions are available for **all devices** configured for use with Privileged Access Manager:

### Device Record Updates

#### *Editing a Device*

To edit the information of a device, select the Device from the **Manage Devices** page. In the device information screen, update the device information as needed, and select the **Save** button.

### ***Copying a Device***

The permissions and policies of an existing device can be copied to create a device with the same access.

To create a Device **ID** by copying an existing device, select the **Copy** button next to the Device ID intended to be used as a template. A copy of the device information is displayed. Add the required fields and make any appropriate changes. Select the **Save** button to create the Device. Associations and policies can be changed after the device is created.

### ***Deleting a Device***

To delete a particular device, select the Device from the **Manage Devices** page. In the device information screen, select the **Delete** button and select the appropriate response on the subsequent confirmation screen.

### **Manage Tags**

Tags, which are created within a Device create/edit template, are compiled by Privileged Access Manager into a list which spans all Devices.

#### ***View Tags***

Select the **Devices**, **Manage Devices**, **Manage Tags** link to display the **Manage Tags** shadow window. All tags are shown (paginated, if needed) with the number of occurrences in the right column.

- Search tags on the **Tag Name** (alphabetically).
- Sort tags on the **Tag Name** (results list alphabetically) or on **#Used** (occurrences) (results list from low to high).

#### ***Edit Tags***

Each tag can be edited or deleted in the Manage Tags window (not in the Create Device / Edit Device template). Select the Tag line item to open an editing box.

### **Manage Groups**

The **Manage Groups** page displays all the groups which have been configured.

### **Manage Services**

In the **Services** tab, the following management options are available.

#### ***Editing a Service***

To change a setting on a service:

1. Select the **Edit** button next to the service.

An Update service screen appears to allow parameters other than the name to be changed.

To change the *name* of a service:

1. Use **Copy** to clone the service attributes (while allowing the Service Name to be filled in).
2. **Delete** the original.

#### ***Copying a Service***

1. From the list in **Services**, **Manage TCP/UDP Services**, open the record of an existing Service.
2. At the bottom of the record, select the **Copy** button.  
A new record is created, populated with a copy of the original Services information except for the Service Name. This new record opens immediately below the record of the copied Service. The record of the copied Service is closed. To confirm this, look at the Service list above the new record editing pane. It should show the line item of the original Service.
3. Enter (the required) Service Name for the new Service. Edit other fields as desired, and select the **Save** button to create the Service.

## ***Deleting a Service***

Select the checkbox next to the service, and select the **Delete** button at the bottom of the screen. The Service is immediately removed, and the remaining Service list appears.

## **Device Viewing**

### **Initial Unfiltered View**

The first time that you access Manage Devices, you see an empty-list page view. The page is labeled "Unfiltered" because the list (initially empty) is shown without filters that are applied.

See [Filtered Views](#) for information about filtering.

### **Unfiltered Views**

From the **Devices**, **Manage Devices** menu, all current devices (initially) appear in alphabetical order by Device Name. You can also sort the list by clicking on any of the displayed field names: Name, Address, OS, Description, or Location; or by applying filters.

Global Settings, Default Page Size determines how many Devices are listed on each Manage Devices page. If there are more Device records than this value, the Manage Device list is paginated, with navigation controls at the bottom of the page.

### **Filtered Views**

The gray-field **Search** function in the upper-right corner of the page body performs the following actions:

- Accepts a non case-sensitive string
- Matches the string to the beginning of the Name field across all Device records
- Replaces what was an Unfiltered list with a new list. The new list is labeled "Filtered"

### ***Fields Available for Filtering***

When the Search box is clicked, a set of three pop-up windows appears at the right under the Search field. Each window contains a list of the unique values (in alphanumerical order) for each of the following Device record fields:

- Device Type
- OS (Operating System field)
- Location
- Tags

If no item is selected, no value is filtered against that field, so all records are shown. Selecting a value in the field, however, filters the set of Device records against that value. Only those records with the selected value are (immediately) shown in a revised list. If multiple values are selected, records that match any of the selected values is included. Any combination of the checkbox selections or strings from each Device field list can be selected for any particular search. For string selections in **OS**, **Location** and **Tags**:

- To select a **sequence** of values in one category: Select the first entry, then while holding the **Shift** key, select the last entry.
- To select any combination of **individual** values in one category: Select one entry after another while holding the **Ctrl** key.



## **Saved Views**

The filtering that you apply can be saved as a View, and used either by default or selected from a menu.

1. After applying desired list filtering, near the top left (to the right of "Unfiltered"), select **Save as View**. The **Save View** pop-up window appears.
2. Specify a label (**View Name**) to use.
3. Select **Set as Default** if you want the Manage Devices page to open to this view by default.
4. Select **Save New View**.

The view is relabeled to the saved view name, and the view can be selected at any time from the **My Views** menu to the left of the Search box.

## **Set Up Access to a Target Device**

You can access a target device from the appliance in one of these ways:

- **Access Method** – If you select an access method, the appliance invokes a proprietary Java applet to connect to a device. The connection uses one of several standard protocols (SSH, RDP, others)
- **Service** – If you select a service, the appliance invokes a local third-party application that resides on your client system. For example, your local Windows PC might be using PuTTY or WinSCP to handle a connection to a Linux target device.
- **RDP Application** – If you select an RDP application, the appliance uses the RDP protocol to invoke a specific application on a target Windows OS Device

The following topics describe the access types for connecting to a target device:

- [Access Methods](#)
- [Create TCP/UDP Services to Access a Device](#)
- [RDP Applications Configuration](#)
- [How to Set Up Auto-Login for Windows RDP](#)

## **Access Methods**

Access Methods are the out-of-the-box communications applets that provide connectivity and session recording. The applets support VNC, TELNET, SSH, RDP, and serial connections. You can change default ports and you can disable protocols for the whole system. Access method applets are downloaded from PAM to a local computer and rely on locally installed Java.

Configuring an Access method is a two-step process:

1. Select the Access Method from the Global Settings menu in the UI.
2. Assign an access method to one or more target devices.

This topic describes the following information and tasks:

### **Select Access Methods**

1. Select **Settings, Access Methods**.
2. Select the methods to be made generally available for a device configuration.  
If you do not want to use a particular access method, clear the checkbox it to disable it. If you disable a particular access method, it is unavailable for all devices.

### **RDP Client Applet Security Requirement**

If you select the RDP Client applet, the applet supports TLS 1.2 connections and the applet supports the TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 cipher suite. The RDP Client also supports forward secrecy using the following supported cipher suites:

- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

For the highest level of security, ensure your RDP target device, that is the Windows server, is configured to use forward secrecy with TLS 1.2 communication.

#### NOTE

If PAM is operating in FIPS mode, but the RDP server does not offer a FIPS-compliant communication option, you receive an error. The error says "Cannot connect to *target\_server* because the server did not offer a FIPS-compliant option for communication." Ask your Administrator to verify the server configuration.

### Customize Access Methods

You can customize the access method. Changes apply globally.

#### Follow these steps:

1. Go to **Settings, Access Methods**.
2. Select an access method to customize, and select **Update**.
3. Modify the settings.  
If you update the default ports, only one port number can be specified per Access Method. No port ranges are allowed.
4. Select **OK**.

The set of Access Methods available depends on which license you have. You must have a mainframe license for the TN applets to be available. Otherwise, those applets do not appear as options.

### Assign an Access Method to a Device

The following procedure assumes you already configured a target device.

#### To assign an access method to a device:

1. From the UI, select Devices, Manage Devices.
2. Double-click the target device entry to open it.
3. Select the **Access Methods** tab.
4. Add an Access Method by selecting the plus sign. In the Name column, select an Access Method from the field drop-down list.
5. Select **Save and Configure Target Applications**. Repeat as necessary to allow more methods to be used.  
You can remove any entry by selecting the X at the end of the entry row.
6. When you finish adding methods, and making other changes to the Device record, select the **Save** button.

### Set Up File Transfer Capability (Optional)

Some access methods need further configuration for functionality, such as file transfers. PAM supports file transfer to and from remote target devices through the SSH access method using the Mindterm applet. File transfers can be recorded. SCP and SFTP protocols are supported. SSH file transfer is globally enabled or disabled on a per PAM appliance basis.

#### NOTE

The MindTerm applet command line window has a 512-column by 512-row limit. If you require a larger window, use PuTTY with [TCP/UDP Services](#).

### Enable SSH Terminal File Transfer (Administrator)

To set up file transfers using the SSH applet:

1. Log in to the UI as an administrator with privileges to access global settings.
2. Navigate to **Settings, Global Settings, Applet Customization**.
3. Select the **SSH Terminal File Transfer** checkbox.
4. Select **Save**.
5. Set up a policy for a PAM user to use the SSH as the access method for applicable target devices.

### Accessing a Target Device using the SSH Access Method (User)

After SSH terminal file transfers are enabled, the user has access to the SCP and SFTP file transfers.

The following procedure explains how a PAM user selects the SSH access method:

1. Log in to the UI as a User with permissions to execute the SSH access method.
2. If necessary, navigate to the Access page.
3. On the Access page, select an **SSH** icon to open a MindTerm applet to the configured target device.
4. In the MindTerm Java applet window (labeled with your device name), select **Plugins, SCP File Transfer** to open a file transfer window.
5. Use the **MindTerm – SCP *internal\_IP\_address*** applet file transfer window to perform the following functions:
  - Move files between your local client computer and the remote target Device. Use the arrows to move between directories in the list.
  - Use the following commands to execute tasks between the two system directories:
    - **Double-click: [..]** – to jump to the parent directory, or *directory\_name* to enter it.
    - **ChDir** – to specify a directory to jump to
    - **MkDir** – to create a directory
    - **Rename** – to change the name of the selected directory
    - **Delete** – to delete the currently selected file or directory
    - **Refresh** – to reload the current directory

### Logging for File Transfer Transactions (Optional)

This table describes the types of log entries that are effected by file transfer transactions.

UI Button	Log Entry Syntax	
	Transaction	Log Entry Details
-->	put	Upload <i>localpath/filename*</i> (size) to <i>remotepath/filename</i> as user <i>remote_user</i> .
<--	get	Download <i>localpath/filename*</i> (size) from <i>remotepath/filename</i> as user <i>remote_user</i> .
		*A directory (with or without files) can also be copied, but that action is not logged. Files within copied directories are each copied and logged.
<b>ChDir</b>	(no log entry)	
<b>Delete</b>	alert	[Remote   Local] [file   folder] <i>pathname</i> has been deleted by user <i>remote_user</i> .
<b>MkDir</b>	alert	[Remote   Local] folder <i>pathname</i> has been created by user <i>remote_user</i> .

<b>Refresh</b>	<i>(no log entry)</i>	
<b>Rename</b>	alert	[Remote   Local] [file   folder] <i>path/old name</i> has been renamed to <i>path/new name</i> by user <i>remote user</i> .

## Create TCP/UDP Services to Access a Device

Configure TCP/UDP services to define local (to the client system) third-party applications that can be used to access a target device instead of a predefined access method. Examples of such clients include:

- PuTTY: For PuTTY or another SSH client, see [Create an SSH Service to Access a Device](#).
- IBM TN3270 and TN5250 clients: See [Set Up a Native TN3270 or TN5250 Client](#).
- Web Portal: To provide access to websites automatically, see [Configure a Service to Access a Web Portal](#).
- SQL query front ends, mainframe clients, and other proprietary applications that use TCP or UDP connections: see [Configure a TCP/UDP Service](#)

You can also import Services in batch mode using a CSV file. See [Import or Export Services](#) for instructions.

### Configure a TCP/UDP Service

To add a TCP/UDP Service, follow these steps:

1. Select **Services, Manage TCP/UDP Services**.
2. Select **Add** to create a new TCP/UDP service.
3. On the **Add TCP/UDP Service** dialog that opens, complete the following fields as appropriate:

- **Service Name:** Enter a name for the customized service.
- **IP Version:** Allows the user to select the IP version: **IPv4** or **IPv6**.

#### NOTE

If this service is associated with a target device that will be used by a PAM Agent, the **IP Version** setting must match the type of IP address that is configured in the target device definition.

- **Local IP:** If you select IPv4, enter a local IPv4 address for this service. The **Local IP** column on the TCP/UDP Services page lists the existing IP addresses for other services.  
If you select IPv6, this step does not apply because ::1 is the only valid loopback address for the IPv6 protocol.
- **Ports:** Define all ports that the client application opens to gain access to the device, using one of these formats:
  - **Port combination/redirection** syntax: **RemotePort:LocalPort** or **RemotePort:\*** (separated by a colon)  
**RemotePort** is on the destination device. Specify an integer.  
**LocalPort** is the local port over which the listener waits for connections on the local user desktop. Enter an \* (asterisk) to let Privileged Access Manager set the value to any available port. Always specify an \* (asterisk) for the local port in Citrix XenApp environments. To enter a specific port number, enter an integer.  
Example: 22:\*  
Example: 22:8855
  - **Multiple ports** syntax: Each port is separated by a space, comma, or comma and space.  
Example: 67 3450 23  
Example: 5740, 3221, 31225
  - **Port range** syntax is: **FirstPort–LastPort** (minimum and maximum value that is separated, by dash). The port range limit is 500. A single range is allowed.  
Example: 14575–15004

Do not combine multiple ports with port ranges. Use only one entry type. The following example is incorrect:  
51000-51002, 55555

- **Protocol:** Select the transport protocol that the service uses from the drop-down list.
- **Enable:** Select this option to enable the service. Disabled services appear shaded in the Devices page, and do not work for any user, including *super*.
- **Show in Column:** Select this option to show the service as a button on the Access page. Otherwise, Services appear in a drop-down list, which is more compact.
- **Application Protocol:** Select one of the following protocols for communication to the remote target:
  - **Disabled** (Default) Accept this value to create a simple pass-through tunnel connection to the remote target.

#### NOTE

The service can be configured so that an application on the client is invoked when the tunnel is built.

- ICA
- RDP
- VNC
- Console
- SSH
- TELNET
- Web Portal

For some application protocols, contextual controls appear. For more information about specific controls for SSH, TELNET, and Web Portal application protocols, see the following topics:

- [Create an SSH Service to Access a Device](#)
- [Create an RDP Proxy Service to Access a Device](#)
- [Set Up a Native TN3270 and TN5250 Client](#)
- [Configure a Service to Access a Web Portal](#)

- **Hide Credential:** (Available when **Application Protocol** is set to **Disabled**.) Set this option to hide the **View Credential** link that is otherwise displayed when a user selects the corresponding service icon on the **Access** panel, as shown in the following screenshot:

- **Send keep-alive interval:** (Available when **Application Protocol** is set to SSH or TELNET.) Select this option to send keep-alive messages so that sessions do not time out. *The PAM Applet Timeout still applies.* Valid values are 60 seconds (minimum) to 172800 seconds (48 hours). Default is 0 (disabled mode). For more information about the Applet Timeout setting, see [Basic Settings](#). For additional information about how this option affects SSH services, see [Create an SSH Service to Access a Device](#).
- **Client Application:** To invoke the client automatically, specify the file path to its executable. The path that you specify here is launched when a user accesses the service. The user can also set or override this path at

launch time. To use a path that requires embedded spaces, enclose the directory path, including the application executable filename, in quotation marks. Do not enclose the entire string in quotes or the command does not execute.

Use these literal strings as variables that Privileged Access Manager substitutes:

- <Local IP> is replaced with the IP address in the **Local IP** field. Do not repeat the local IP here.

#### NOTE

If you are using IPv6, the <Local IP> in the command line must be surrounded with square brackets: [<Local IP>]

- <First Port> is replaced with the first local port (after the colon) that is defined in **Ports**. Do not repeat the first port here.
- <User> is replaced with the account name that is used in the access method. Do not repeat the account name here.
- <Second Port> is replaced with the second local port (if any) that is defined in **Ports**. Do not repeat the second port here.
- <Device Name> is replaced with the Name of the Device. Some application connection arguments can use this variable. For example, in WinSCP, /sessionname=<Device Name> displays the device name instead of the IP address in the application title bar.

For Example: If WinSCP is the application on the client, enter the following path:

"C:\Software\WinSCP\WinSCP.exe" scp://<User>:<Password>@<Local IP>

**Important!** In the WinSCP example, use the literal strings <User>, <Password>, and <Local IP>. Do not enter the actual values for these strings.

#### NOTE

The <Password> variable poses a security risk. It exposes the password to the client, which might log it or might expose it as an argument. When the user connects, a "View Credential" link is shown. You can mitigate this risk by configuring the [Password View Policy](#) with the **Change Password On View** option.

4. Select **OK**.
5. Create a Device that corresponds to the target device.
  - a. In **Devices, Manage Devices**, create a Device with the target IP address (do not use FQDN) in the **Address** field.
  - b. On the **Services** tab, use the controls to move the service that you created from the Available Services to the Selected Services.
  - c. Select **OK**.
6. Create a **Target Application** using the target device as **Host Name**. See [Add Target Applications](#) for more information.
7. Create a **Target Account** using the target application as **Application Name**. The **Account Name** is substituted for <User> and the **Password** for <Password>. See [Add Target Accounts](#) for more information.
8. Create a **Policy** linking the Target Device to a User or Group.
  - a. On the **Services** tab, select the Service that you created.
  - b. In the **Target Account** column, use the Edit magnifying glass icon to select the Account.

The Service appears on the **Access** page for the select User or Group.

#### **Additional information:**

- [Create an SSH Service to Access a Device](#)
- [Set Up a Native TN3270 and TN5250 Client](#)
- [Configure a Service to Access a Web Portal](#)
- [Import or Export Services for Access](#)

## Create an SSH Service to Access a Device

An SSH Service invokes a local third-party SSH application on a client to connect to a device. The target device does not have to host the SSH application, and it must reside on the user client computer. This feature extends the access control to any native SSH client. This feature allows control to include session recording, socket filtering, command filtering, and automatic connection with the target account.

### NOTE

When a native SSH client service policy is configured for session recording, select the **Bidirectional** checkbox for the recording to work.

Follow these steps:

1. Select **Services, Manage TCP/UDP Services**.
2. Select **Add** to create a new TCP/UDP service.
  - **Service Name:** Enter a name for the service.
  - **Local IP:** Enter a valid local loopback address.
  - **Ports:** Enter **22** (for SSH) and a local port mapping or an asterisk. For example: **22:12345** or **22:\***
  - Enable option the **Enable**.
  - Select the **Show in Column** option to display the service as a button on the **Access** page. Otherwise, Services appear in a drop-down list, which is more compact.
  - For **Application Protocol**, select the **SSH** option from the drop-down list. Configure the following SSH-specific controls that appear, as required:
    - **SFTP or SCP.** (Optional) For more information, see [Enable File Transfer](#) in the next section.
    - **Optionally, select X11.** (Optional) Select this option to enable the X11 protocol for the user interface. For more information, see [X11 Forwarding and Command Execution](#).
    - **Public Key Authentication.** (Optional) For more information, see [Enable Public Key Authentication](#).
    - **Send keep-alive interval:** (Optional) Send keep-alive messages so that sessions do not time out. (The PAM Applet Timeout still applies.) Valid values are 60 seconds (minimum) to 172800 seconds (48 hours). Default is 0 (disabled mode). For more information about the Applet Timeout setting, see [Basic Settings](#).  
This option also changes how SSH rekey operations, background jobs, and activity in SSH sessions (such as running commands like `top` that update the terminal at regular intervals), impact the applet timeout functionality of PAM. See the following table for examples of how this setting behaves in relation to the rekey operation.

Keep Alive Setting	If Rekey > Applet Timeout		If Rekey < Applet Timeout	
	Background Job	Activity in SSH	Background Job	Activity in SSH
0 (Disabled)	Timeout	No timeout	No timeout	No timeout
Keep-alive is less than applet timeout (overrides original the timeout behavior)	Timeout	Timeout	Timeout	Timeout
Keep-alive is greater than applet timeout	Same as 0 (Disabled)			

3. **Client Application**, enter the path if you want to invoke the client automatically.
4. The Client application path that you specify here is launched when the enabled SSH service is accessed.

Windows syntax:

```
C:\[path]\[clientApp].exe [options] <User> <Local IP> <First Port>
```

For PuTTY:

```
"C:\Program Files\PuTTY\putty.exe" -ssh -l <User> <Local IP> <First Port>
```

Linux syntax:



```
/usr/bin/putty -ssh -l <User> -P <First Port> <Local IP>
```

#### MacOS syntax:

- If you are using IPv4, enter the following command or the terminal app:

```
open -n -a "Terminal" ssh <User>@<Local IP> -p <First Port>
```

- If you are using IPv6, enter the following command or the terminal app:

```
open -n -a "Terminal" ssh <User>@[<Local IP>] -p <First Port>
```

Use these literal strings as variables that Privileged Access Manager substitutes:

#### NOTE

If you are using IPv6, the <Local IP> in the command line must be surrounded with square brackets: [<Local IP>]

- <Local IP> is replaced with the IP address in the **Local IP** field. Do not repeat the local IP here.
  - <First Port> is replaced with the first local port (after the colon) that is defined in **Ports**. Do not repeat the first port here.
  - <User> is replaced with the account name that is used in the access method. Do not repeat the account name here.
  - <Second Port> is replaced with the second local port (if any) that is defined in **Ports**. Do not repeat the second port here.
  - <Device Name> is replaced with the Name of the Device. Some application connection arguments can use this variable. For example, in WinSCP, "/sessionname=<Device Name>" displays the device name instead of the IP address in the application title bar.
  - Privileged Access Manager automatically inserts the password, so there is no need to provide it.
5. Select **OK**.
  6. Create a Device that corresponds to the SSH target you want to connect.
    - a. In **Devices, Manage Devices**, create a Device with the target IP address (do not use FQDN) in the **Address** field.
    - b. On the **Services** tab, use the controls to move the service that you created from the Available Services to the Selected Services.
    - c. Select **OK**.
  7. Create a **Target Application** using the target device as **Host Name**. See [Add Target Applications](#) for more information.
  8. Create a **Target Account** using the target application as **Application Name**. The **Account Name** is substituted for <User> and the **Password** for <Password>. See [Add Target Accounts](#) for more information.
  9. Create a **Policy** linking the Target Device to a User or Group.
    - a. On the **Services** tab, select the Service that you created.
    - b. In the Target Account column, use the Edit magnifying glass icon to select the Account.

The SSH Service appears on the Access page for the select User or Group.

### Enable File Transfer

You can configure a TCP/UDP SSH Service to do the file transfer operations for a native SFTP or SCP application. Session recording is not activated when either of these features are invoked.

### **Administrator Setup**

You can set up your native SSH Service to allow one of the following options: Automatic Invocation or Manual Invocation.

### **Prerequisites**

To use the file transfer over SSH service, verify that the SSH server on the target Device is configured to provide SFTP sub-system or SCP execution.

### **Automatic Invocation**



Automatically invoke the SSH application with options through the Privileged Access Manager Service command-line specification (in the **Client Application** field) when selecting the service link.

### Manual Invocation

Manual invocation of the SSH application by the user, who applies commands at execution. To invoke the application, select the service link on the Access page.

### User Experience

#### Automatic Invocation

A user on a properly configured client invokes an Access page Service link. The SFTP or SCP client executes automatically with the specified switches or commands. After logging in or auto-connecting to the target device, the user can execute the file transfer operations such as uploading or downloading functions that are provided by the native SFTP or SCP client application.

#### Manual Invocation

If the Privileged Access Manager Service **Client Application** setting is empty, the User starts a local SFTP or SCP client application manually to execute the SFTP or SCP connections.

### Log Entries

A session log entry is written each time a file transfer operation is executed. The following operations are written to a session log:

- Uploading a file to the target device
- Downloading a file from the target device
- Deleting a file on the target device (SFTP only)
- Creating a folder on the target device (SFTP only)
- Removing a folder on the target device (SFTP only)

### Supported SFTP and SCP Client Software

- Windows: WinSCP, FileZilla, Putty
- Mac: FileZilla, OpenSSH (SCP only)
- Linux: OpenSSH (SCP only)

For the FileZilla client, PAM supports the official release version and does not support the development version.

## X11 Forwarding and Command Execution

You can configure a TCP/UDP Service to do X Window System (X11) forwarding and command execution for a native SSH application.

### NOTE

Session recording is not activated when either of these features are invoked.

### Administrator Setup

You can set up your native SSH Service to allow one of the following options:

- Automatically invoke the SSH application with options through the Privileged Access Manager Service command-line specification (in the **Client Application** field)
- Manual invocation of the SSH application by the user, who applies commands at execution. To invoke the application, select the service link on the Access page.

### Prerequisites

To use X11 forwarding, verify that the target Device has X11 applications that are installed. Also confirm that the SSH server that is configured to provide X11 forwarding. The User workstation must run an X11 server to display the output.

**NOTE**

When used on UNIX, Linux, and other UNIX-like systems, the SSH Access Method requires the **socat** relay utility.

**Automatic Invocation**

To configure an SSH session so that it automatically invokes a client application with X11 forwarding, set the X11 option.

**Manual Invocation**

If a TCP/UDP Service is configured to use SSH without specifying the **Client Application**, the user can manually invoke any installed application, such as PuTTY. The service can then use the X11 forwarding or command execution options available to that application.

**User Experience****Automatic Invocation**

A user on a properly configured client invokes an Access page Service link. The SSH client (PuTTY) executes automatically with the specified switches or commands.

1. After logging in or auto-connecting to the target, the User can immediately run X11 applications on the target. The application output is forwarded to the workstation.
2. If a command is specified, the session immediately closes when the command is finished executing.

**Manual Invocation**

If the Privileged Access Manager Service **Client Application** setting is empty, the User must start a local SSH client application manually to execute the SSH connection. The User uses that application X11 forwarding or command execution features. For example, after invoking PuTTY on a Windows workstation, you would use PuTTY **Connection, SSH, X11, Enable X11 forwarding** or **Connection, SSH, Remote** options, respectively. If a command is specified (using the latter option), the session immediately closes when the command is finished executing.

**Log Entries**

A session log entry is written each time an X11 forward occurs or a command is executed for this feature.

**Enable Public Key Authentication**

You can configure a TCP/UDP Service to connect to a target device using the Public Key Authentication method for a native SSH Application.

**Administrator Setup****Prerequisites**

On the native SSH Application: To use Public Key Authentication, verify that the native SSH application enabled **Public Key Authentication** and enabled **Agent Forwarding**.

On the Target Device: Confirm that the SSH server is configured to authorize the public key of the user in their authorized key file (\$HOME/ssh/authorized\_key) or an equivalent file.

**NOTE**

When authenticating using the public key of the user, confirm that Privileged Access Manager has no auto-login configured under Policies.

You can set up the native SSH Service to allow one of the following options:

**Automatic Invocation**

Automatically invoke the SSH application with options through the Privileged Access Manager Service command-line specification (in the Client Application field).

To configure an SSH session so that it automatically invokes a client application with agent forwarding, set the agent forwarding option.

For PuTTY: -A option. For example: C:\apps\putty72\putty.exe -ssh -A <Local IP> <First Port>

### Manual Invocation

Manually invoke the SSH application by enabling agent forwarding. To invoke the application, select the service link on the Access page. Then, launch the native SSH application.

If a TCP/UDP Service is configured to use SSH without specifying the **Client Application**, the user can manually specify the public key authentication and agent forwarding in any installed application, such as PuTTY, and then open a connection. The service can use the public key authentication and agent forwarding options available to that application.

### User Experience

#### Automatic Invocation

A user on a properly configured client invokes an Access page Service link. The SSH client executes automatically with the specified switches. The user can immediately connect to the target using the public key authentication method.

#### Manual Invocation

If the Privileged Access Manager Service **Client Application** setting is empty, the user must start a local SSH client application manually to execute the SSH connection. The user uses that application public key authentication and agent forwarding. For example, after invoking PuTTY on a Windows workstation, use the **PuTTY Private key file for authentication** and **Allow agent forwarding** settings.

### Log Entries

A session log entry is written when trying to do a public key authentication without enabling this feature.

- Public Key Authentication is not permitted over the SSH TCP service. Contact your system administrator.
- Agent forwarding is required to connect using a public key over the SSH TCP service.

## Set Up a Native TN3270 and TN5250 Client

Create a TCP/UDP Service to invoke a local third-party application on a client to connect to a device. The target device does not have to host the client application, which must reside on the user client computer. Native TN3270 and TN5250 client support extends the access controls to any native IBM host client. These controls include session recording and automatic connection with the target account setup. Services and clients must be of the same type for session recording to work. For example, you must configure a TN5250 service to be used with a TN5250 client.

### NOTE

In a PCOMM client, negotiation for the function `CONTENTION-RESOLUTION` is enabled by default. When this function is enabled, session recording fails. You can disable the function by adding the following keyword to the .WS profile:

```
[Telnet3270] TN3270EContentionResolution=N
```

### Follow these steps:

1. On the **Basic Info** tab, enter values for the following fields:
  - Service Name:** enter a name for the portal.
  - Local IP:** enter a valid local loopback address.
  - Ports:** enter 23 (for TN3270 or TN5250) and a local port mapping or asterisk. For example: **23:12345** or **23:\***
  - Select the **Enable** checkbox.
  - For the **Application Protocol**, select **TELNET** from the drop-down list.
2. Select a **Mainframe Protocol** from the drop-down list.

For the **Client Application**, enter the path if you want to invoke the client automatically. The path that you specify here is launched when the enabled SSH service is accessed. Use the syntax in the sample line. Use or substitute the tags as identified here.

**Windows:** C:\path\clientApp.exe [options] username@<Local IP> <First Port>

<Local IP> is submitted and replaced with the IP address in the **Local IP** field.

<First Port> is replaced by the first Local port (after the colon).

Example for a Client Application specification: "C:\Downloads\QWS 3270\QWS3270.exe" <Local IP> <First Port>

When setting up a service for a mainframe proxy, use this execution path as an example:

C:\Program\putty.exe -ssh <Local IP> <First Port>

Some clients may require this syntax: C:\Program\TN5250.exe -ssl:<Local IP>:<First Port>

3. Select **OK**.
4. Create a Device that corresponds to the target device.
  - a. In **Devices, Manage Devices**, create a Device with the target IP address (do not use FQDN) in the **Address** field.
  - b. On the **Services** tab, use the controls to move the service that you created from the Available Services to the Selected Services.
  - c. Select **OK**.

#### NOTE

We recommend that all mainframe connections terminate by selecting the "Disconnect" option in the terminal emulator, not by directly shutting down the terminal emulator application.

#### WARNING

When a native TN3270 or TN5250 client service policy is configured for session recording, select the **Bidirectional** checkbox for the recording to work.

## Configure a Service to Access a Web Portal

Configure the Web Portal application protocol to access websites automatically. This application automatically launches a new browser window and navigates to a preset local IP and launch path.

#### NOTE

Establish a portal for every web server that the user accesses. Some servers provide content to the web pages that call them (through embedded links) but do not face users. See the **Hide From User** option.

#### WARNING

**Warning:** VMware NSX API is no longer supported as of PAM 3.3.

#### Follow these steps:

1. Select **Services, Manage TCP/UDP Services**.
2. Select **Add** for a new TCP/UDP service.
3. For **Service Name**, enter a name for the customized service.
4. For **Local IP**, enter a valid local loopback address.

#### WARNING

To set up a Web Portal for Microsoft SharePoint® and Mac client access, set the **Local IP** to 127.0.0.1 and provide a valid **Host Header**.

5. For **Ports**, enter **80** (for HTTP) or **443** (for HTTPS). Optionally, specify a local port mapping. For example, add **:8080** to map **Remote:Local** as **80:8080**
6. Select the **Enable** checkbox.
7. For **Application Protocol**, select the **Web Portal** option from the drop-down list.

8. **Auto Login Method** defaults to "Disabled." If you specify an automatic login method, such as SAML 2.0 SSO POST, two new tabs activate. For more information, see [How to Configure Automatic Login to Web Portals](#).
9. Enter a value for the **Launch URL** field. The URL specified here is launched when the web portal enabled service is accessed. Use the literal phrases "<Local IP>" and "<First Port>", which use the values in the **Local IP** and **Ports** fields. Use the following syntax: `http[s]://<Local IP>:<First Port>/path_to_target_page`
  - <Local IP> is a literal placeholder for the IP address in the **Local IP** field. Do not repeat the local IP address here.
  - <First Port> is a literal placeholder for the first local port (after the colon) that is defined in **Ports**. Do not repeat the first port here.
  - `path_to_target_page` is the path component of the URL. Create any legal subdirectory path, including:
    - `[directory/[subdirectory/[...]] ]` - optional directory path
    - `[terminal_component.ext]` - optional terminal page/program

Examples:

```
http://<Local IP>:<First Port>/index.html
https://<Local IP>:<First Port>/dashboard.jspa
```
10. Select the **Browser Type**:
  - **Native Browser**: Invoke a window to the Web Portal using the same browser that the User has used to access **Privileged Access Manager** instance.

**NOTE**  
The Symantec PAM Browser is required for web portal recording. The Symantec PAM Browser is also required for all Auto-Login methods except SAML 2.0 SSO POST.

  - **PAM Browser**: Invoke a custom restricted-function browser. PAM Browser is required for web portal recording and all Auto-Login methods except SAML 2.0 SSO POST.
11. Specify the applicable FQDN hostname in **Host Header** so that the portal is able to distinguish between multiple hosted websites, for example, `www.example.com`. If the IP address of the server hosts only one (FQDN) site, this field is not required. However, it is good practice to specify it explicitly.
  - Host Header is not applicable to HTTPS (SSL) sites.
  - Host Header is required for Microsoft SharePoint sites.
  - Host Header applies to a native browser only.
12. If any alias host names are used to reach the portal, enter these names in the **Aliases** field. Separate the names with commas. These aliases are mapped by Privileged Access Manager to the true host (see Host Header). This field applies to a native browser only.
13. If the portal is to be used in the background, select **Hide From User**. This option specifies that a server is available for Privileged Access Manager-internal access, but is not to be accessible to an end user. For example, a server that delivers graphic files that are requested from a browser after a baseline website delivers an HTML page. This field applies to a native browser only.
14. An **Access List** applies to the PAM Browser only. In the **Access List** field, include each host to which access is allowed. A good practice is to examine session logs to find blocked access attempts.
  - a. Enter one host per line.
  - b. An asterisk acts as a wildcard. For example: `*.ca.com`
  - c. Exclude any hosts that pose security risks.

**NOTE**  
In addition to hosts listed in the access list, the web portal can access any device configured in PAM which has an access policy that includes both the web portal itself and the user, whether directly or through groups.
15. Select the **Route Through Symantec PAM** checkbox so that all traffic is directed through Privileged Access Manager. Otherwise, traffic goes directly to the web service from the client workstation. Web Portal traffic can be recorded even if **Route Through Symantec PAM** is not selected.
 

**NOTE**  
The **Native Browser** option does not allow PAM session recording. The user must still select the **PAM Browser**.
16. Select **OK**.

17. Create a Device that corresponds to the web server you are aiming to reach. In Devices, Manage Devices, create a Device with the web server IP address (do not use FQDN) in the **Address** field.

### Next Step

- [How to Configure Automatic Login to Web Portals](#)

## How to Configure Automatic Login to Web Portals

You can create services that manage access to web portals. You can set up manual login or automatic login. This topic describes how to set up automatic login to web portals.

The following methods are available to log a user into a target web portal automatically:

- **PAM HTML Web SSO:** Use this option when the login method that the web portal employs is HTML-based. This method is the most common.  
As a web page is loaded into the PAM Browser, a JavaScript injection provides credentials to the web page HTML, then executes the login. This method requires that the administrator "teach" PAM which login page widgets to use. Some widgets capture the username and the password while another widget acts as the login trigger. Examples of web portals that use this method include Dropbox and Google.
- **PAM HTTP Web SSO:** Use this option when the login method that the web portal employs is the HTTP protocol. In this case, PAM encodes login credentials and inserts them into a header. The header is appended onto each HTTP or HTTPS request. Examples of web portals that use this method include Microsoft SharePoint installations.
- **Built-in Auto-Login Methods:** Built-in methods are also available. These built-in methods allow automatic login-in with the following specific web portals:
  - VMware vCloud Director
  - VMware vShield Manager
  - VMware vSphere Web Client v5; the VMware vSphere Web Client v5 auto login method is only suitable for vSphere v5. To configure auto login for vSphere Web Client 6.0, see [Automatic Login to vSphere Web Client 6.0 Configuration](#).

## Configure a TCP/UDP Auto-Login Service

Create a TCP/UDP auto-login service that is associated with the web portal.

### Follow these steps:

1. Navigate to **Services, Manage TCP/UDP Services**.
2. Select **Add** to create a TCP/UDP service.
3. On the **Add TCP/UDP Service** dialog that opens, complete the following fields as appropriate:
  - **Service Name:** Enter a name for the customized service.
  - **IP Version:** Allows the user to select between IPv4 or IPv6.
  - **Local IP:** If IPv4 is selected, enter a local IPv4 address for this service. The **Local IP** column on the TCP/UDP Services page lists the existing IP addresses for other services.  
If IPv6 is selected, this step does not apply since the value is automatically hard-coded to ' : : 1 ' .
4. For **Ports**, define the ports or port range that the client application opens to gain access to the device. Example: 8000
5. For **Application Protocol**, select Web Portal.  
More options appear on the right side of the page.
6. For **Auto-Login Method**, select the appropriate method, as described previously:

- **PAM HTML Web SSO** is best suited to websites that have user name and password entry fields. This method requires administrator configuration using the Learn Tool.
  - **PAM HTTP Web SSO** is best suited to websites that receive user names and passwords programmatically, such as through Windows Authentication. This method does not require using the Learn Tool.
  - **SAML2.0 SSO POST** requires information about the web portal SAML attributes. [See Set Up SAML 2.0 SSO POST for Auto-Login](#) for more information.
7. For **Launch URL**, follow the example URL. To access the URL `https://www.forwardinc.com/login.html`, replace the target login address (`www.forwardinc.com`) with the target template `<Local IP>:<First Port>`. The resulting entry is: `https://<Local IP>:<First Port>/login.html`
  8. For **Browser Type**, select CA PAM Browser to enable session recording.
  9. For **Access List**, enter \* (an asterisk) as a wildcard. The **Access List** indicates the URLs that can be accessed along with the launch URL. During the Auto-Login, to login to the web portal, the launch URL is followed by other URLs pertaining to the response of login. Therefore, to Auto-Login to the web portal, the **Access List** must be either "\*" or each host that is allowed access.
  10. Select **OK** to save the service.

### **Assign the Auto-Login Service to a Device**

Add the newly created service to the device hosting the web portal. The device is then available for a policy. See [Device Setup](#) for more information about configuring a device.

#### **Follow these steps:**

1. Select **Devices, Manage Devices**.
2. Add the target device hosting the web portal.
3. Select the **Services** tab then select the new TCP/UDP service that you defined.
4. Select **OK**.

### **Create a Target Application, Target Account, and Policy**

Configure a target application and account for the web portal. Completing these tasks enables the storage of credentials. The policy ties the users and the device together to access the web portal automatically.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**, then complete the following fields:
  - **Host Name:** Use the magnifying glass **Select** icon to find and select the host name of the device hosting the web portal.  
**Device Name** is automatically populated.
  - **Application Name:** Enter a descriptive application name.
  - **Application Type:** Accept the default, Generic.
3. Select **OK** to save the target application.
4. Select **Credentials, Manage Targets, Accounts**.
5. Select **Add**, then complete the following fields:
  - **Application Name:** Use the magnifying glass **Select** icon to find and select the application.  
**Host Name** is automatically filled.
  - **Account Name:** Enter the name of the account (user name) for logging in to the web portal. For example: **admin**.
  - **Password:** Enter the password for the account.
6. Select **OK** to save the target account.
7. Select **Policies, Manage Policies**.



8. Select **Add** and set up a policy that associates an existing user or group to the device that hosts the automated login service.
9. On the **Services** tab, select the Service that you created.
10. In the Target Account column, use the Edit magnifying glass icon to select the Account.
11. Select **OK**.

If your target website uses the PAM HTML Web SSO method, you must configure a "learn" procedure to activate the portal for end users.

### **Set up a Learn Procedure for PAM HTML Web SSO**

For target websites that use the PAM HTML Web SSO method, perform a "learn" procedure to activate the portal for end users. An HTML auto-connection portal requires that the HTML field and button widgets be identified. These settings capture a login username and password and activate the browser to submit the username and password for login processing.

#### **Follow these steps to set up the Learn procedure:**

1. Log in to the PAM UI.
2. Go to the **Access** page. A Web Portal drop-down is now available with two services for this device, for example, **MyApp (LEARN)** and **MyApp**.
  - The **Learn** option shows a red **X** to its left. The administrator uses the Learn option to contact the login address and teach the service to recognize the target widgets. After the setup is successful, the red **X** changes to a green checkmark. The checkmark indicates that access to the web portal is activated and is ready to use.
  - The **Login** option is for the actual login entry. The administrator must successfully apply the learn mode *first* for the login service to function.
3. Select the **Learn** option.  
The learn tool launches the target web portal page, but you cannot log in. The window name in the browser title bar is prefaced with "Learn mode for Web SSO."
4. For the service to use widgets for auto-login, teach the service where the widgets are located:
  - a. Right-click in the **User Name** (or other name identifier) field to open the learning menu.
  - b. Select **Mark Accountname Field**.  
The field is populated with the placeholder field "accountname ."
  - c. Right-click in the **Password** field and select **Mark Password Field**.  
The field is populated with an obfuscated password.
  - d. Hover over the button to log in then right-click to select **Mark Submit Button**.
  - e. For any other required widgets for your portal, perform the required action for each widget. (There is no right-click menu item to select, and there is no feedback, but all action is recorded.)

For example, to teach the service to learn the interface to another site, target the portal that requires LDAP authentication. In addition to teaching the service about the three widgets, select "LDAP" for the **Authentication Type** setting. Also, select the appropriate configured domain from the list. All these actions are preserved for auto-connection when you save them.
5. In the upper-right corner of the browser window, select the Save **auto-login template** disk icon.  
The configuration is saved and the browser window closes.
6. Repeat the learning process at any time to save new results.
7. Return to the **Access** page. The learning option now has the green checkmark, indicating that the Learn option is complete.

When an end-user logs in to the UI, the **Access** page now has a single access link without the learn-mode option. The user selects that link and gets auto-logged on to the target web portal.



## Set Up SAML 2.0 SSO POST for Auto-Login

You can set up automatic login to third-party web portals that support SAML SSO, such as Google.com. To configure many of the SAML SSO information fields and attributes for the Web Portal, you must refer to the third-party SAML provider instructions. Ideally, you want to import SAML 2.0 SP metadata from the provider as XML. See [How to Configure the Product as an Identity Provider \(IdP\)](#) for detailed information about setting up SAML authentication, including examples for AWS and Google applications.

See [Configure a TCP/UDP Auto-Login Service](#) for instruction on configuring the **Basic Info** tab of a TCP/UDP Service. When you select SAML 2.0 SSO POST as the **Auto-Login Method**, two tabs become active.

1. On the **Basic Info** tab, use the Web Portal **Entity ID** as the **Service Name**. This value is often a domain name.
2. For the **Auto Login Method**, select SAML 2.0 SSO POST.  
The SAML SSO Info and SAML SSO Attributes tabs become active.
3. In the **Launch URL** field, enter the Assertion Consumer Service (ACS) URL of the RP. The ACS URL is a combination of the PAM web portal URL root and the ACS URL. For example, the web portal URL root is: "https://local\_ipfirst\_port". The ACS URL is: `https://capamAsSp.example.com/samlsp/module.php/saml/sp/saml2-acps.php/capam-default-sp`  
Resulting Launch URL is:

```
https://111.12.123.21:239/samlsp/module.php/saml/sp/saml2-acps.php/capam-default-sp
```

4. Leave the **Route Through Symantec PAM** checkbox selected. This option directs all traffic through PAM. When this option is not selected, traffic goes directly to the web service from the client workstation.
5. On the **SAML SSO Info** tab, enter the following information from the third-party RP:
  - **SAML Entity ID:** This ID is typically a domain name.
  - **Initiating Party:** Select which partner initiates the call.
    - **SP Initiated** (default): If the user logs in to the SP/RP first, an authentication request is sent to the IdP to obtain the assertion. The returned assertion allows the SP to make a service access decision. (SAML 2.0 only)
    - **IdP Initiated** – The user logs in to the IdP to initiate connection and to obtain the assertion for a service at an SP.
  - **Require Signed Authn Requests:** This checkbox is selected by default. The SP must sign the authentication request that it sends to the IdP. To verify the signature, specify the supplied PEM signing certificate, gkcert.crt. in the PEM Signing Certificate field.
  - **Encryption:** By default, encryption is not enabled. Select whether PAM encrypts, the Name ID or the Assertion, then paste the base64 translation of X.509 certificate encryption certificate in the **PEM Encryption Certificate** field.  
Example: `<ds:X509Data> <ds:X509Certificate>encodedContent</ds:X509Certificate>`
6. On the **SAML SSO Attributes** tab, select the appropriate **SAML SSO Subject Name Identifier Formats** for your web portal. If your provider requires an attribute that is not listed, provide the attribute in the **Add a new SAML SSO Attribute** section. Complete the fields for each entry.
  - Name: Specify the attribute name.
  - Friendly Name: assign a name or tag for use by the appliance. If the imported SP metadata does not provide the friendly name, the entry for the Name field is used.
  - Required: Select if the SP requires this attribute.

### NOTE

You might have to add a SAML mapping on the **SAML** tab of the Policy configuration.

7. Select **OK**.
8. Follow the instructions in [Assign the Auto-Login Service to a Device](#).
9. Follow the instructions in [Create a Target Application, Target Account, and Policy](#).

## Automatic Login to vSphere Web Client 6.0 Configuration

To configure automatic login to vSphere Web Client 6.0, use the following settings when completing the previous procedures:

- **Port:** 443
- **Auto-Login Method:** PAM HTTP Web SSO
- **Launch URL:** `https://<Local IP>:<First Port>/vsphere-client`
- **Address:** Specify the vSphere server domain name. An IP address does not work. Example:  
`vcenter.north.afc.nfl.local`

## Import or Export Services for Access

As a Privileged Access Manager administrator, you can import or export Services using a CSV file. You can import three types of services in one file, from any of their respective pages:

- TCP/UDP Services
- RDP Applications

To create or edit services by importing a CSV file:

1. Select **Services**, and either Manage TCP/UDP Services, or Manage RDP Applications.
2. Select the **Import/Export** button.  
The Import/Export window appears.
3. Select **Download Sample File** to save a template file to a convenient editing location.
4. Copy the sample to a new file, and open it in a spreadsheet program or a plain-text editor.

### NOTE

**Microsoft Excel** incorrectly interprets the colon-embedded fields that are intended to be used as *RemotePort:LocalPort* representation. Cell E7 contains "4.815972..." This is an Excel conversion of the original plain-text CSV content that is provided in the file, namely, "23:5555". Even if adjustments are made to the Excel and file save-as settings, this behavior persists in reading or writing the file.

### Workarounds

- a. Always use plain-text editor (for example, Notepad) to prevent conversions from occurring.
  - b. Use Excel first for most editing. As a final editing stage, open the file in a plain-text editor, and delete any conversions. Repopulate those cells with colon-embedded values such as *RemotePort:LocalPort*.
5. Edit or add line items for each service desired and save the file. For descriptions of each field, see [CSV Files for Services](#).

### NOTE

Do not to alter the first (header) line.

6. Select **Choose File** to browse for your saved CSV file.
7. Select **Import Services**.

To export a CSV file of you existing services, follow these steps:

1. Select **Services**, and either Manage TCP/UDP Services, or Manage RDP Applications.
2. Select the **Import/Export** button.  
The Import/Export window appears.
3. Select the **Export Services** button to export a CSV file.

## Create an RDP Proxy Service to Access a Device

An RDP Service invokes a local third-party RDP application on a client to connect to a device. Native RDP Client support extends the Access controls to any native RDP client.

The RDP proxy configuration requires the RDP application configuration.

The RDP proxy service supports the following Privileged Access Manager policies:

- Socket-filtering
- Auto-login
- Session-recording
- Transparent-login

To Create an RDP Proxy Service, follow these steps:

1. Select **Services, Manage TCP/UDP Services**.
2. Select **Add** for a new TCP/UDP service.
  - **Service Name:** Enter a name for the service.
  - **Local IP:** Enter a valid local loopback address.
  - **Ports:** Enter **3389** (for RDP) and a local port mapping or an asterisk. For example: **3389:12345** or **3389:\***
  - Protocol should remain set to TCP.
  - Select the **Enable** checkbox.
  - Select **Show in Column** to show the service as a button on the Access page. Otherwise, Services appear in a drop-down list, which is more compact.
  - For **Application Protocol**, select the **RDP** option from the drop-down list.
3. **RDP Application:** Select a previously configured RDP Application Service that enables you to launch Transparent Login using the RDP Proxy service. To configure an application service, go to Services, Manage RDP Applications service. This option only appears when you select RDP as the application protocol.
4. **Learn Mode:** Check this box to provide an option on the Access page to launch Learn Mode using the RDP Proxy Service. During Learn Mode, Privileged Access Manager is taught the credential-processing interfaces of the provisioned RDP application. This process captures the required sequence in a transparent login configuration file that is stored in Privileged Access Manager. When you check this option, the Show In Column is also enabled, which shows a drop-down arrow on the RDP service displayed on the Access page. When you click on the arrow, you can launch the service with or without Learn Mode enabled. the drop-down arrow enables you to differentiate between services which have Learn Mode enabled and which do not on the Access Page. The Learn Mode drop-down arrow is only shown on the Access page for users with Global Administrator or Service Manager privileged and is hidden for all other users. This option only appears when you select RDP as the application protocol.
5. For **Client Application**, enter the path if you want to invoke the client automatically
6. The path that you specify here is launched when the enabled RDP service is accessed.

Windows remote desktop application:

If you are using IPv4, enter the following command:

```
C:\<path>\mstsc.exe <options>/v:<Local IP>:<First Port>
```

If you are using IPv6, enter the following command:

```
C:\<path>\mstsc.exe <options>/v:[<Local IP>]:<First Port>
```

For macOS:

If you are using IPv4, enter the following command:

Microsoft RDP:

```
open -a "Microsoft Remote Desktop" rdp://full%20address:<Local IP>:<First Port>
```

If you are using IPv6, enter the following command:

Microsoft RDP:

```
open -a "Microsoft Remote Desktop" rdp://full%20address:[<Local IP>]:<First Port>
```

These literal strings are substituted at run-time:

- <Local IP> is replaced with the IP address in the **Local IP** field. Do not repeat the local IP here.

#### NOTE

If you are using IPv6, the <Local IP> in the command line must be surrounded with square brackets.

- <First Port> is replaced with the first local port (after the colon) that is defined in **Ports**.

7. Select **OK**.
8. Create a Device that corresponds to the RDP target device that you want to connect to.
  - a. In **Devices, Manage Devices**, create a Device with the target IP address (do not use FQDN) in the **Address** field.
  - b. On the **Services** tab, use the controls to move the service that you created from the Available Services to the Selected Services.
  - c. Select **OK**.
9. Create a **Target Application** using the target device as **Host Name**. See [Identify Target Applications and Connectors](#) for more information.
10. Create a **Target Account** using the target application as **Application Name**. The **Account Name** is substituted for <User> and the **Password** for <Password>. See [Add Target Accounts to Target Applications](#) for more information.
11. Create a **Policy** linking the Target Device to a User or Group.
  - a. On the **Services** tab, select the Service that you created.
  - b. In the Target Account column, use the Edit magnifying glass icon to select the Account.

The RDP Service appears on the Access page for the select User or Group.

### Administrator Setup

You can set up your native RDP Service to allow one of the following options:

- Automatically invoke the RDP application with options through the Privileged Access Manager Service command line specification (in the **Client Application** field)
- Manual invocation of the RDP application by the user, who applies commands at execution. To invoke the application, select the service link on the Access page.

### Manual Invocation

If a TCP/UDP Service is configured to use RDP without specifying the **Client Application**, the user can manually invoke any installed application, such as mstsc.

### User Experience

#### Automatic Invocation

A user on a properly configured client invokes an Access page Service link. The RDP client (mstsc) launches automatically.

## Configure RDP Applications Templates

Configure an RDP application template to access Windows-hosted applications that have enabled RDP access. Assign that template to a device.

#### Follow these steps:

1. Select **Services, Manage RDP Applications**.
2. Select **Add** and complete the following information:
  - **RDP App Name:** Specify a unique name (up to 255 characters) for the RDP application service.
  - **Launch Path:** Enter the full path to the RDP application that runs after the user connects to it. The Launch Path field is case-sensitive, so pay attention to capitalization.  
For example: C:\Windows\System32\notepad.exe

You can enter an AWS URL to specify the AWS Management Console home page. This token is used as the target address of a browser on a recording-designated Windows “jump box.”

3. Select **Enable** to make this application available to Privileged Access Manager devices.
  4. Optionally, select the **Hide From User** check box so the RDP Application link is not displayed on the Access page.
  5. Optionally, select the **Transparent Login** tab and select the **Transparent Login** check box. Transparent login allows for the passing of vaulted credentials to applications hosted on a remote Windows server. A direct link to the RDP Application, which bypasses the Windows shell, is prevented. Transparent login credential handling (automatic login to the application target) for this application in an RDP session is still enforced.
- The **Application Fingerprint** field is optional. When using the Learn Tool, Specify the SHA-1 digest for the application obtained when using the Learn Tool. The product uses this digest value when the user accesses the application. For more information about Transparent Login, see [Set Up Transparent Login](#).

## Configure Auto-Login for Windows RDP

Learn how to configure Windows RDP access to a target device so that the end user logs in automatically without entering a password.

Complete the following procedures to configure Auto-Login for Windows RDP.

### Watch a Video

Watch this video to see a demonstration of this topic.

### Create a Device

Add the device to which you want to provide auto-login access. For more details about Device attributes that are not covered in this procedure, see [Device Group Setup](#).

#### Follow these steps:

1. Select **Devices, Manage Devices**.
2. To specify a new device, select **Add**.
3. Enter a **Name**. This name is displayed on the Access page. You can enter double-byte characters.
4. Enter the device IP address or FQDN in the **Address** field.
  - For FQDN, DNS must be set up properly on the **Configuration, Network, Network Settings** page.
5. For **Device Type**, select Access and Password Management.
6. Select **Scan** to detect services that are configured on the device. The detected services appear on the Access Methods and Services tabs. RDP should appear on the Access Methods tab after selecting **Scan**.
7. Select **OK** to save the Device.

### Create an Application

Add the Application and Target Connector for connecting users to your device. For Windows RDP, you can use one of the following connectors. Select an Application Type according to your Windows infrastructure and the type of login account you plan to use.

- [Windows Proxy Connector](#): To use the Windows Proxy connector, you must install the connector on a remote server in your target domain.
- [Windows Remote Target Connector](#): The Windows Remote target connector uses local Windows accounts to connect.
- [Active Directory Target Connector](#): The Active Directory connector uses Active Directory accounts to connect.

For ease of demonstration, we use the Windows Remote connector.

**Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Use the **Host Name** magnifying glass to find the target device. Select the device and select **OK**.
4. The **Host Name** and **Device Name** of the target server are populated.
5. Enter a unique **Application Name**. This name does not have to be an existing application on the target device.
6. In the **Application Type** field, select **Windows Remote**.
7. Select the **Windows Remote** tab.
8. For the **Account Type**, select **Local Account**. This type is only able to manage local accounts on target servers.
9. Select **OK** to save the Application.

**Create an Account**

Add the login account for Privileged Access Manager to use to log in to the target device. For more information about setting up accounts for different application types, see the following pages:

- [Windows Proxy Target Accounts](#): The Windows Proxy connector can use local accounts or domain accounts with the AD connector.
- [Windows Remote Target Accounts](#): The Windows Remote target connector uses local Windows accounts to connect.
- [Active Directory Target Account](#): The Active Directory connector uses Active Directory accounts to connect.

For ease of demonstration, we use the Windows Remote connector.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. The Target Account page appears with a list of existing accounts.
2. Select **Add**. The Add Target Account page appears.
3. Select the **Application Name** magnifying glass to find the target application. Select the application and select **OK**. The **Host Name**, **Device Name**, and **Application Name** fields are populated.
4. Enter the **Account Name**. The account name must be unique for a given target application and must be the account name that the target system uses.
5. Select the **Password View Policy** for the account.
6. Enter an initial account **Password** or select the Generate Credential key icon to generate a default password.
7. On the **Password** tab, Select **Discovery Allowed** to discover accounts on the Windows remote system.
8. Select the **Update both the Credential Manager Server and the target system**. Password updates are performed both in Credential Manager and on the target system to maintain consistency.
9. On the **Windows Remote** tab, select the Administrator **Account Type**.
10. Select **OK** to save the Account.

**Create a User**

Add a User that you want to use auto-login to access the target device. For information about authentication methods, roles, and other User attributes, see [Identify Users that Can Log in to the Server](#). For ease of demonstration, we create a "local" Privileged Access Manager user.

**Follow these steps:**

1. Select **Users, Manage Users**.
2. Select **Add** to create a user.
3. Complete the required fields in the **Basic Info** section (indicated by a red asterisk).
  - **User Name** accepts alphanumeric characters, a dash, an underscore, and spaces. For AWS users, a user name can be from 2 through 32 characters long because of restrictions on federated users within AWS.
4. Select **OK** to save the User.

## Create a Policy

Create a Policy linking the user, the device, and the account. For more detailed information about policies, see [Set Up a Policy](#).

### Follow these steps:

1. Select **Policies, Manage Policies**.
2. Create a policy by clicking **Add**.
3. Use the fields in the **Association** tab to locate the user and device that you want to associate in the policy. Select the search icon in each field to display the list of choices. Select an entry and **OK** to add it to the Association screen.
4. On the **Access** tab, select "RDP" and move it to the Selected Access list. Then select the target account that you created for auto-login. Use the magnifying glass button under the Target Account heading to find the account. Use the shuttle control to move the account from the Available column to the Selected column.
5. Select **OK**.
6. If [session recording capability is configured](#), you can specify the types of recording to make using the options on the **Recording** tab.
7. Select **OK** to save the Policy.

The User should now be able to log in to the Access page, and RDP into the Device without credentials.

## Manage Command and Socket Filters

In the PAM UI, select **Policies, Manage Policy Filters** to configure the following policy filters:

- [Command filters to prevent commands that you specify from executing and socket filters](#)
- [Socket Filter Lists \(SFLs\) that define the sockets to which a Socket Filter Agent allows or denies access.](#)

### Set up Command Filters

Command filters are access restrictions that prevent commands that you specify from executing. You configure command filter lists to enforce a policy in the command line applets TELNET, SSH, and serial consoles. Command filters do not work on Windows Devices.

#### Next Steps

- [Set up Command Filter Lists \(CFL\)](#)
- [Set up Command Filter Configuration \(CFC\)](#)

#### NOTE

For information about setting up Socket Filters, see [Socket Filter Agent Support](#).

### Set up Command Filter Lists (CFL)

Command filtering, like Socket Filters, uses whitelists and blacklists to set the appropriate policy.

- A **blacklist** is a list of commands that a user cannot type. If the user attempts to type the command, Privileged Access Manager can flag (log), alert, remediate, and stop the command from being processed. All other commands are allowed.
- A **whitelist** is a list of the commands that a user can type. All other commands are prohibited.

#### NOTE

Command filter whitelists cannot be configured for Mainframe TN3270 and TN5250 applets.



Create Command Filter Lists (CFLs) in the user interface using the CFL template or by importing a CSV. See [Import or Export Command Filter Lists](#) for information about importing a socket filter list with a CSV.

### Use the CFL Template

Use the following procedure to create and manage Socket Filter Lists using the SFL template. Follow these steps:

1. Select from the Menu Bar: **Policies, Manage Policy Filters.**
2. The **Command Filters** page appears.
3. Select the **ADD** button.  
The **Add Command Filter** window appears.
4. Enter a **Name** for this socket filter list.
5. Specify the **Type** of list:
  - A **Blacklist** denies only the listed command strings.  
If a user submits a CLI command to a device that is on the blacklist, the user request is denied. This denial applies **per character**: After sufficient characters (literal Keyword or Regexp) are entered match a violation criterion, the specified action (Alert/Block) is applied. You must configure a policy for this user that specifies the blacklist.
  - A **Whitelist** allows access only the listed command strings.  
If a user submits a CLI command to a device that is on the whitelist, then those commands are allowed. This allowance applies **per line string entered**. The permission test is made following a linefeed/Enter/carriage return. You must configure a policy for this user that specifies the whitelist.

#### NOTE

Command filter whitelists cannot be configured for Mainframe TN3270 and TN5250 applets.

6. Select the plus icon to Add a new Keyword.
7. In the **Keyword** field, enter a command string. Depending on which type of list you are creating:
  - a. If you are creating a **blacklist**, then for each Keyword to test, you must select one or more controls:
    - **Alert** – Select this box to alert Monitoring administrator immediately by email with each instance of Keyword violation.
    - **Block** – Select this box for the command line containing the Keyword to be canceled immediately, and prevented from executing.
    - **Regexp** – Select this box if the Keyword field specifies a regular expression to be applied to the actual command entered. Whenever a command that is entered by the User conforms to the regexp, the command is flagged as a violation.
    - When both **Regexp** and **Alert** are selected, the body of the alert message does not include the Keyword regular expression string for security reasons.

If the **Keyword** is a regular expression and not simply a literal character match, then you must select the **Regexp** checkbox. There is no action taken unless you select either **Alert** and/or **Block**.

#### NOTE

Alert and Block log the violation in the sessions log of the local node where the violation occurred. For example, if a standard user commits a violation after having logged into their access method from a secondary site node in a cluster, that violation is only logged in the sessions log of that particular secondary site cluster node. Furthermore, if you want to receive email on the Alerts, you must have the Admin Email configured and the Monitor started on the particular cluster node where the violation occurred. See [Set Up Email for Monitoring](#) for more details.

**Important:** When populating the Keyword field for a **blacklist** using **Regexp**, begin with a start-of-line metacharacter, typically **^**. However, because a blacklist keyword string is evaluated character by character, the end-of-line metacharacter (ordinarily: **\$**) is never interpreted and is therefore unnecessary.

**Example:** Match (prevent) a user key entry of exactly **who -a**

Fill the Keyword field with one of the following regular expressions:



- Correct: **^who -a**
- Correct: **^who -a\$**

However, each of the following regular expressions does *not* work correctly:

- Incorrect: **who -a**
- Incorrect: **who -a\$**

b. If you are creating a **whitelist**, then for each Keyword to test, you can select:

- **Regex** – Select this box if the Keyword field specifies a regular expression to be applied to the actual command entered. The regular expressions that are permitted follow the syntax that is supported by the Perl-based Oracle® `java.util.regex` API. The command succeeds only when it conforms to one or more of the regex or commands in this whitelist.

When populating the Keyword field for a **whitelist** when using **Regex**, it does not matter whether you include the start-of-line (ordinarily: `^`) or end-of-line (ordinarily: `$`) metacharacters. These metacharacters are implied. The string that the user enters is automatically anchored by both of these metacharacters.

**Example:** Match (allow) a user entry of exactly: **who**

Enter Keyword field content of any of the following regular expressions:

- Correct: **who**
- **^who**
- **^who\$**
- **who\$**

**Example:** `[LI][Ss] +`

This regular expression permits variations of uppercase or lowercase on the UNIX command **ls**, but requires that a space be added for the expression to be accepted.

**Example:** `[LI][Ss] +\-[LIAa][LIAa]?`

This regular expression is a variant of the previous example, which is based on **ls -al**, in which uppercase and lowercase are again permitted. But the order of the two characters **al** is arbitrary, and two or more spaces are required between the command and its argument. Because the command filter string is anchored by start-of-line and end-of-line metacharacters, trailing spaces are prohibited in this example.

8. Select the **OK** button to save the settings.

The list is now effective in Privileged Access Manager, and available for inspection or editing to the Command Filter list page.

## Search Command Filter Lists

You can search existing command filter lists for matches to a character substring by using the **Search** field. This search flags a list when there is a match in its **Name** field, and when there is a match in any of the **Keyword** fields for that list.

## Import or Export Command Filter Lists

Use the following procedure to create and manage command filter lists using a CSV file.

### Follow these steps:

1. Go to **Policies, Manage Policy Filters**.  
The **Command Filters** page appears.
2. Select the **Import/Export** button.  
The Import/Export command filters window appears.
3. A sample file is available by selecting the **Download Sample File** button. Copy the sample file to a new file, and edit it for your use.
4. All columns are required fields. See [Set up Command Filter Lists \(CFL\)](#) for detailed information about these fields.

- **Type:** Command Filter List
  - **List Name:** This text populates the **Name** field on the Command Filters list page.
  - **List Type:** white or black  
Use "white:" for a Whitelist, which is a list of commands that a user may use. All other commands are prohibited.  
Use "black:" for a Blacklist, which is a list of commands that a user may not use. All other commands are permitted.
  - **Keyword:** Enter the command or command subset to be restricted. Multiple commands for the same list are designated by multiple CSV line items using the same List Name.
  - **Alert:** t or f for true or false  
If true, immediately notify the monitoring administrator of any use of this command.
  - **Block :** t or f for true or false  
If true, this command is canceled and prevented from executing.
  - **Regexp :** t or f for true or false  
If true, the Keyword field is evaluated as a regular expression when matching a command. If there is a match, apply any Alert or Block specified.
5. Use the **Choose File** button to select the completed CSV file for import and select **Import Command Filters** to upload.  
The list is now effective, and available for inspection or editing on the **Command Filters** list page.

### WARNING

If you include a blacklist line in the CSV file with the same key fields (**Type**, **List Name**, **List Type**, and **Keyword**) found in an earlier line, the latter line replaces the earlier line. The values that are applied for **Alert**, **Block**, and **Regexp** are the last values read, or the values in the last key-matching line.

### Export Command Filters

Use the **Export Command Filters** button to export existing SFLs to a CSV file. These lists can be stored, modified, and imported or reimported later.

### Set up Command Filter Configuration (CFC)

This screen is used to create and manage command filtering.

1. Select from the Menu Bar: **Policies, Manage Policy Filters**.  
The Command Filters page appears.
2. In the upper corner of the white page body, select the **CONFIG** link.  
The Command Filter Config template appears.
3. Adjust the fields where necessary, and click **OK** to save the settings.

### Command Filter Configuration Pane

Field	Description
Messages	

Blacklist Violation Message	<p>The default is: Warning: [command] is an unauthorized command. You have [violations] violations. Your session will be terminated and account deactivated should violations continue. Contact the administrator if you have any questions ... where "[command]" is substituted during execution with the string (keyword) used, and "[violations]" is substituted during execution with the number of (including the current) occurrences of this violation by this user (and "[newline]" is substituted with a line feed).</p> <p><b>Note:</b> Double-byte characters such as those used for traditional Chinese are permitted.</p>
Whitelist Violation Message	<p>The default is: Warning: [command] is an unauthorized command. Contact the administrator if you have any questions ... where "[command]" is substituted during execution with the string (keyword) used (and "[newline]" is substituted with a line feed).</p> <p>NOTE Double-byte characters such as those used for traditional Chinese are permitted.</p>
Violation Additional e-mail Message	<p>This area is provided for information that is sent to the configured administrator if violations occur. (No default is provided.) NOTE Double-byte characters are NOT permitted in email messages. (They are permitted only in screen messages.)</p>
<b>Action</b>	
# Violations Before Action	<p>The numerical value of the number of violations that are permitted to occur. When the violation count matches the threshold, the action in the Action After Limit Exceeded is taken. Set this value to zero (0) if no count is enforced. The count of violations is on a per session basis regardless of how many times the user connects.</p>
Action After Limit Exceeded	<p>Select the appropriate action that complies with policy when the user exceeds the number of violations.</p>

## Socket Filter Agent Support

Socket Filter Agents (SFAs) are components that you can deploy to restrict access to and from server-based devices. SFAs are installed on a remote target device. For information about downloading and installing Socket Filter Agent software, see [Install and Configure a Socket Filter Agent](#).

Socket filters apply rules that are used in access policies. These rules are specified by configuring socket filter lists from the PAM UI.

### NOTE

If an SFA is installed on a Windows system, the SFA filters do not get applied to VNC connections.

To configure SFA lists and policies, follow these procedures:

### Create a Socket Filter List

A Socket Filter List (SFL) defines the sockets to which a Socket Filter Agent allows or denies access. An SFL can be a whitelist or a blacklist:

- **Blacklist:** A blacklist denies access only to the listed services and ports. A user can request access to a device with a policy that has this blacklist. Any user that requests a socket on this list is denied access. The user is allowed access for sockets that are *not* on the blacklist.
- **Whitelist:** A whitelist allows access only to the specified servers and ports. A user can request access to a device with a policy that has a whitelist. Any user that requests a socket that is on this list is allowed access. The user is denied access for sockets that are *not* on the whitelist.

Create an SFL using one of the following methods:

- Use the SFL template in the UI. Use the procedure in this topic.
- Import a CSV file. For instructions on how to import a CSV file and create an SFL, see [Import or Export Socket Filter Lists](#).

#### TIP

To ensure proper performance, define no more than 8000 sockets in each SFL.

#### Follow these steps to create a filter list:

1. From the PAM UI, select **Policies, Manage Policy Filters**.  
The **Policies** page appears.
2. Select the **Socket Filters** tab.
3. Select the **Add** button.  
The **Add Socket Filter** window appears.
4. Enter a **Name** for this socket filter list.
5. Specify the type (blacklist or whitelist) in the **Type** field.
  - When used against LDAP users, socket filter whitelists must also include IP addresses of the relevant domain controller or controllers. IP addresses can change in your environment, so whitelists can require active management. You might have to update the filters.
  - For PKI smartcard users, socket filters must be actively managed.
6. Select the plus sign (+) to add a new host.
7. Enter the IP Address and ports to filter. The **Ports** field is limited to 512 characters.

#### NOTE

If a host has both IPv4 and IPv6 addresses, you must add a host entry for each address.

8. Select **OK** to save the settings.

The list is now effective, and available for inspection or editing with the **Socket Filters** list page.

#### Configure a Socket Filter Policy

#### NOTE

Do not configure VNC access to log in to a Windows system installed with an SFA. This access method does not work with a Windows SFA.

#### Follow these steps:

1. From the PAM UI, select **Policy, Manage Policy Filters**.
2. Select the **Socket Filters** tab.
3. Select the **Config** button.  
The **Socket Filter Config** pane appears, populated with default values.
4. On the **Basic Info** tab, inspect these settings:
  - **Agent Port**  
The agent port must match the port where the agents are listening. The default is 8550.
  - **SFA Monitoring**

Select this box to enable monitoring socket filter agents. Agent status appears on the Devices, Socket Filter Agent page. Enable this option if policies disallow users to log in to a device if an agent is not running.

- **Appliance ID**  
Set a unique number (from 1 to 254) for each physical appliance, especially in a cluster. This ID is required for using SFAs with Windows.
  - **Log All Access**  
Select this box to log all access activity, whether a device is on a whitelist or it is missing from a blacklist. Second-generation Socket Filter Agent installation is required.
5. On the **Messages** tab, inspect these settings:
- **Violation Message**  
Customize the message ("Access is denied") that appears to the user when a policy is violated. The following strings (including brackets) are substituted as specified:  
[host] is Replaced by the IP address of the blocked host.  
[port] is Replaced by the port of the blocked connection.
  - **Violation Additional e-mail Message**  
Add text area for information that is sent to "super" if violations occur.**Prerequisite:** Administrator email must be configured.
- Double-byte characters are NOT permitted in email messages. They are permitted only in screen messages.
6. On the **Action** tab, inspect these settings:
- **Number of Violations Before Action**  
Set the number of violations that are permitted to occur. When the violation count matches this threshold, the action that is specified in Action After Limit Exceeded is taken. Set this value to zero (0) if no count should be enforced.  
The count of violations is persistent per user-device basis regardless of how many times the user connects. Thus a user is not permitted to reset the count by reconnecting and trying again.
  - **Action After Limit Exceeded**  
Select the appropriate action to comply with policy when the user exceeds the number of violations.
7. Select **OK** to save the settings.

### **Enable Socket Filter Agent Monitoring**

To enable monitoring of SFA Agents, follow these steps:

1. Navigate to **Policies, Manage Policy Filters, Socket Filters**
2. Select **Config**.
3. Select the **SFA Monitoring**.
4. Select **OK** to save your settings.

### **View Socket Filter Agent Status**

The appliance runs a scan at regular intervals to determine the status of all SFAs. After you enable SFA monitoring, you can view the status of the SFAs.

To see the list of SFAs:

1. Navigate to **Devices, Socket Filter Agent**. The Socket Filter List Status page displays.  
You only see entries on this page if you enabled monitoring.
2. Look at the **Status** column. The column shows one of the following values:
  - **Active:** The SFA is up and running. The appliance is able connect to the Agent on port 8550 of the remote host.
  - **Inactive:** The SFA was active but not for the past few minutes.
  - **Unknown:** The SFA was active but has not been active for an extended period of time. Reasons why the SFA might be unreachable are that the Agent is turned off, disabled, or uninstalled.

## Import or Export Socket Filter Lists

Use the following procedure to create and manage socket filter lists using a CSV file.

### NOTE

If your CSV file contains duplicate records, only one of the duplicate rows is imported; any others are ignored. For example, if a CSV file contains the following rows, one row is imported and the other row is ignored:

Type	List Name	List Type	IP Address	Port
Socket Filter List	whiteList	white	1.2.3.4	80
Socket Filter List	whiteList	white	1.2.3.4	80

### Follow these steps:

1. Go to **Policies, Manage Policy Filters**.  
The **Socket Filters** List page appears.
2. On the **Socket Filters** tab, select the **Import/Export** button.  
The Import/Export socket filters window appears.
3. A sample file is available by selecting the **Download Sample File** button.
4. All columns are required fields.
  - a. **Type:** Socket Filter List
  - b. **List Name:** This text populates the **Name** field on the Socket Filter List page.
  - c. **List Type:** white or black  
Use "white" for a Whitelist, which is a list of sockets (IP address and port combinations) that a user may use. All other sockets are prohibited.  
Use "black" for a Blacklist, which is a list of sockets that a user may not use. All other sockets are permitted.
  - d. **IP Address**  
The IP address can be a single address or a mask. All of these example addresses are valid:  
**IPv4:** 192.168.1.14, 192.168.1.14/24  
**IPv6:** fd6d:8d64:af0c:1:0:242:22:233, fd6d:8d64:af0c:1:0:242:22:233/64
  - e. **Port**  
You can include one or more port numbers, comma or space separated, or one port range. All these ports are valid (semicolons not included):  
5555; 0-65535; 5555 7777; \*; 21,22,23
5. Use the **Choose File** button to select the completed CSV file for import and select **Import Socket Filters** to upload.  
The list is now effective, and available for inspection or editing on the **Socket Filters** list page.

### NOTE

To add new socket filters to your existing socket filter list, create and import a *fresh* CSV file that contains only the new entries. The new socket filters are added to the existing list in PAM. Do *not* add the new entries to an existing socket filter CSV and reimport that file. To maintain an up-to-date socket filter list for your records, export the complete list to CSV after importing the new entries.

## Export Socket Filters

Use the **Export Socket Filters** button to export existing SFLs to a CSV file.

## Setting Up Transparent Login

Transparent login enables automated log-in to a remote target application that has been accessed through auto-connection login.

The two services that support transparent login are RDP and SSH.

### **Next Steps**

- [SSH Connections](#)
- [Set Up Transparent Login for RDP Servers](#)
- [Import or Export Transparent Login Configurations](#)

### **Associate Multiple Target Accounts for Use as Transparent Login Credentials**

Within a Policy, you can associate multiple Target Accounts for use as Transparent Login Credentials (TLC) for a Transparent Login enabled RDP Application Service (TL Service). TLC for a Policy containing a TL Service is decoupled from the TL Service Windows. There is no limit to the number of accounts you can select as TLC for a Policy containing a TL Service. This allows you to configure multiple accounts as TLCs for use within RDP sessions. End users can select from that list of TLC when they access the TL Service through the Access page.

This feature allows the use of Stacked Policies. A stacked Policy refers to multiple Policies that are assigned to same user who is a part of different user groups. Previously, the TL service applied a single Policy for the user, and the user could log in using only one TLC.

The functionality enables the user to select any credential that is aggregated across multiple Policies which the user may be a part of.

Multiple TLC can be on the same host device, or on multiple devices. This functionality enables you to select TLC from any applicable device that the user wants to go, and transfers them accordingly. To use this ability, the Transparent Login Configuration should have host="true" in the applicable location.

## **SSH Connections**

From the SSH access method applet, you configure a device to permit execution of **sudo** or **pbrun** commands using the login password for the device.

### **NOTE**

You cannot apply transparent login to Device Groups

### **NOTE**

Transparent login supports the following items at the target device:

- OS versions: UNIX and Linux
- Shell types: bash, csh, tcsh, and ksh
  - The following restrictions apply to the **ksh** shell type:
    - Vi command line history is not supported.
    - Emacs command line history does not support recalling commands. Example: If a command has one or more carriage returns in it, the command runs but cannot be recalled properly in emacs mode.
    - Using Ctrl-C to break a looping command is not supported.
- Applications: sudo and BeyondTrust PowerBroker pbrun

### **WARNING**

Configure sudo or pbrun on the target so that each execution requires a password from the client. Otherwise, security can be compromised

## Unix/Linux Configuration

Configure **sudo** or **pbrun** for target devices to request a password every time that it is invoked. Privileged Access Manager responds transparently to the request. For example, set `timestamp_timeout=0` so that a password is always required. The sudo execution must always require a password or security is compromised.

### Configure Transparent Login for a Device

To configure a Device to allow secondary transparent login, follow these steps:

1. Create or open an existing Device record on the **Devices, Manage Devices** page.  
If this device record is new, populate at least the required attributes (entitled in **red**).
2. In the **Access Methods** panel, select **SSH**.
3. Scroll to the **Transparent Login** panel. Complete the following fields to configure sudo or pbrun (or both):
  - **Full Path to** - Identify the directory location of the sudo or pbrun executable on the target Device.
  - **Password Prompt** - Specify a prompt (or a fully static substring) for user password input that is presented immediately upon executing sudo/pbrun.  
The full prompt that is experienced by the user might be "[sudo] password for *user*: ", where "*user*" represents the dynamically applied actual username. The maximum string that can be applied here is then: "[sudo] password for ", so use that string.
4. Complete configuring of other device fields as needed, and select Save.
5. Create or open an existing policy record on the **Policy, Manage Policies** page.
6. Scroll to the Transparent Login panel and select the checkbox to turn on transparent login. Clear it to turn it off for a particular User/User Group.
7. Complete the provisioning of other Policy fields as needed, and select Save.  
Transparent login is now ready for Access use to this Device.

#### NOTE

You can configure only a *single* account in the transparent login policy for a CISCO device. Multiple accounts are *not* supported in the transparent login policy.

## User Experience

The User logs in as usual to the target Device using the SSH Access Method applet. When sudo or pbrun is enabled, the normal response (prompting the user to enter a password) is not displayed. The product supplies the password for the auto-connection, and sudo/pbrun continues to execute the sudo commands.

#### WARNING

In some uncommon scenarios, transparent login does not behave as intended, and the user experiences unexpected behavior. For example, a token ("XGK####") is visible or a password prompt might appear. In these cases, exit the application by entering a return, or if necessary Control-C. Retry the command, taking care to apply the correct syntax.

### Complex Commands

You can use a configured privileged command (sudo or pbrun) anywhere, and multiple times, on a command line while Privileged Access Manager provides the login password for uninterrupted completion.

Examples:

```
$ for i in $(cat newusers.txt); do sudo useradd $i; done
$ sudo vi /etc/ssh/ssh_config && sudo /etc/init.d/ssh restart
```

You can also use a configured privileged command (sudo or pbrun) on multiple lines while Privileged Access Manager provides the login user password for uninterrupted completion.



Example:

```
$ *for i in $(cat a_remote_location/deep_in_some_subdirectory/*
> newusers.txt); do sudo useradd $i;\
> done
```

### **Unsupported Syntax**

Transparent login does not support the following command uses:

- Sending a sudo command argument to the background, such as:  
\$ sudo updatedb &
- Stringing a sudo command after a vi exit command, such as:  
:wq sudo updatedb

Exit the vi window with the Enter key first.

### **NOTE**

If a password prompt appears during execution of a sudo or pbrun command in a Windows device, exit using Ctrl-C. Any other response might trigger a password lockout, such as pressing Enter or another key entry

### **Audit Logs**

Following each invocation of or pbrun, an audit log entry like the following example is written:

```
2016-03-11 01:16:27      user      xssso      ubuntu      Executed "sudo pwd" using transparent login as username
```

## **Set Up Transparent Login for RDP Servers**

You can implement transparent login for a Windows RDP server. Transparent login provides secondary access through an application on that device. As with Privileged Access Manager HTML WebSSO, the administrator uses "Learn Mode" to teach the product to recognize the relevant access interface of a target application. In this case, it is a Privileged Access Manager-configured RDP Application.

The benefit of the feature is that credentials and software are not stored on the target RDP server. No installation of agents is needed on the access client or the RDP server. Optionally, these applications can be cached for improved load times.

### **NOTE**

#### **Transparent Login with RDP Proxy Fails with Protocol Error**

To use transparent login with an RDP proxy, you must enable drive mapping in the RDP client and disable other device mappings, such as printers, ports, and so on.

Otherwise, no special configuration is required on Privileged Access Manager or the target Device. This provisioning process embodies the required setup.

This topic explains the following information:

### **Target Devices Support**

- **OS versions:** Windows Server 2012, Windows Server 2016, Windows Server 2019; x86 and x64 versions for each
- **Applications:** VMware vSphere Client and vSphere Client console; Microsoft SQL Server Management Studio; WinSCP; Dell Toad; PuTTY; Oracle SQL\*Plus

## **Windows Configuration**

Windows (RDP server) devices that are the targets of Privileged Access Manager transparent login require the following configuration to work properly.

### **Certificates**

If you are using a signed certificate on Privileged Access Manager, you must install the CA certificate on each Windows target Device. Import this certificate as a Trusted Root.

### **Session Recording**

For transparent login activity to be successfully recorded when using Internet Explorer, configure all equivalent Privileged Access Manager addresses. For example, a cluster VIP name and VIP address in the browser security settings:

1. In Internet Explorer, select **Tools, Internet Options**.
2. Select the **Security** tab, then on **Trusted Sites**, and then the **Sites** button.
3. In the **Trusted sites** dialog window, key in and **Add** each equivalent Privileged Access Manager address in use. Select **Close** to exit Trusted sites.
4. Select **OK** to save and exit Internet Options.

This setting might not work fully. If that is the case, try this additional configuration in **Internet Options**:

1. Select the **Connections** tab, then on **LAN settings**. If the **Proxy server** checkbox is selected, select the **Advanced** button.
2. In the **Exceptions** section, remove any "127.\*" or equivalent construct
3. Select **OK** to save and exit **Proxy Settings**. Then, select **OK** again to save and exit **Local Area Network (LAN) Settings**, and then **OK** again to save and exit **Internet Options**.

## **Prerequisites**

### ***On Windows Server 2012***

1. Add your Windows Server 2012 to your Domain.  
For testing purposes, you can instead install a Domain Controller on the same server. See:  
<http://social.technet.microsoft.com/wiki/contents/articles/12370.step-by-step-guide-for-setting-up-a-windows-server-2012-domain-controller.aspx>
2. Install the Remote Desktop Session Host role using the following instructions:  
<https://support.microsoft.com/en-us/help/2833839/guidelines-for-installing-the-remote-desktop-session-host-role-service>
3. Configure cmd.exe as a RemoteApp using the instructions in the following article:  
<http://social.technet.microsoft.com/wiki/contents/articles/10817.publishing-remoteapps-in-windows-server-2012.aspx>  
For security reasons: In the **RemoteApp Properties** dialog, **Command-line arguments** option button, select the **Always use the following command-line arguments** option. Set its arguments to use the following string.  
Whether you copy-and-paste this string or you enter it in manually, ensure that you do not introduce any additional hidden characters or white space. Otherwise, the command might not work.

```
/C title Initializing RDP session&echo Please wait...&timeout 4 /nobreak>nul&"\
\tsc\client\virt\xcd_run.bat"
```

### ***On Windows Server 2016 and Windows Server 2019***

1. Add your Windows Server 2016 or Windows Server 2019 to your Domain.  
For testing purposes, you can install a Domain Controller on the same server. Refer to the following article for guidance:  
<http://pc-addicts.com/setup-dhcp-role-server-2016/>

2. Deploy your Remote Desktop environment, referring to the Microsoft documentation for guidance:  
<https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-deploy-infrastructure>
3. Create a Remote Desktop Services collection for desktops and apps to run. See the following Microsoft documentation for guidance, stopping when you reach the "Publish RemoteApp Programs" section, then proceed to Step 4 in this procedure.  
<https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-create-collection>
4. Follow these steps to publish cmd.exe as a RemoteApp:
  - a. In **Server Manager**, select the new collection
  - b. Under **RemoteApp Programs**, select **Tasks, Publish RemoteApp programs**
  - c. Select **Add**
  - d. In the file chooser, use the search box to locate and select the appropriate instance of cmd.exe
  - e. Select **Open**
  - f. Select **Next**
  - g. Select **Publish**
  - h. Under **RemoteApp Programs**, right-click **cmd** and select **Edit Properties**
  - i. Select **Parameters**
  - j. For security reasons, set the **Always use the following command-line parameters** option and set its arguments to use the following string:
 

```
/C title Initializing RDP session&echo Please wait...&timeout 4 /nobreak>nul&"\\tsclient\virt  

          \xcd_run.bat"
```

**NOTE**  
 Whether you copy-and-paste this string or you enter it manually, ensure that you do not introduce any additional hidden characters or white space. Otherwise, the command might not work.
  - k. Select **OK**

## Configure Windows Transparent Login

Learn how to configure PAM to enable automated log-in to remote Windows target applications.

Complete the following procedures to configure Windows transparent login on and through PAM:

1. [Preparing Target Device records, including an RDP server hosting an RDP Application](#)
2. [Running the Learn Tool at the RDP server in coordination \(through the RDP Access Method applet\)](#)
3. [Configure the RDP Application record](#)
4. [Provision Target Account records and activate PAM policy](#)

### NOTE

To run Learn Tool and edit transparent login configurations, a PAM administrator must have at minimum the role of Service Manager. This level of role permits the `servicesRead`, `servicesManage`, and `servicesDelete` privileges. Among the preconfigured roles, these privileges are also provided only to the Global Administrator and Operational Administrator roles.

This topic also describes the following other related topics:

- [Caching](#)
- [Auditing](#)
- [User Experience](#)

## Prepare Targets

Initially, as the PAM administrator, you provision a Device and the RDP Application that is the target (or intermediary) of the transparent login. You might also want to provision (in Credential Manager) the primary access credentials that

are consumed during login to the Device. At this stage, you do not need to provision the secondary credentials that are consumed by the RDP Application.

## Run Learn Mode

During Learn Mode, PAM is taught the credential-processing interfaces of the provisioned RDP Application. This process captures the required sequence in a transparent login configuration file that is stored at PAM.

## Example Procedure

This example procedure uses the execution of a connection to a Linux target device using the RDP Application PuTTY.

1. Confirm that you have provisioned the required target Device. Confirm that the target RDP Application, that is configured later, is installed on that Device.
2. If needed, log in to PAM as the administrator responsible for Learn Mode.
3. Navigate to the **Access** page.
4. Mouse over the **RDP** link to the target device until the **RDP options** dialog opens and then do the following actions:
  - a. Select the **Learn mode** option.
  - b. Optionally, expand the size of your RDP window in **Resolutions** to the largest practical value. Example: "Fullscreen" Learn Mode is easier to use when there is a large target desktop.
  - c. Select **Launch** to initiate the RDP connection.

Your RDP applet and connection launch.

Following login, a script window appears telling you that the Learn Mode Tool ("Transparent Login Learn Tool") is launching. The initial **Learn Tool** window opens. If transparent login configurations are already set up, they are shown in the drop box near the upper left corner of the Learn Tool.

Use the Learn Tool, to create a configuration script that allows PAM to recognize the username, password, submit, and other widgets of an RDP Application when your users connect to that application. This script also populates and executes these widgets for transparent login.

Initially, several configurations (Transparent Login Configurations, or TLCs) can be pre-populated in PAM. As the Learn Tool is launched, these configurations are loaded into Learn Tool memory and are available from the configuration name drop-down list.

In this example, we create a configuration. First, assign it a name, in this example PuTTY-to-LinuxTarget1. This name is found in the **Transparent Login Configurations** list on PAM. You can edit the name in the **Name** field when you prepare your RDP Application record.

- a. Select the "Add new configuration" button, and in the dialog window enter a **Name**, and select **OK**.  
The configuration name now appears in the field to the left of that button, and is immediately saved.
  - b. To save the (currently empty) configuration in PAM with this name, select the "Save configuration" button.
5. Open your target RDP application; a configuration interface is ordinarily presented (the **PuTTY Configuration** window).  
While both the Learn Tool and the application are open during this procedure, you populate the Learn Tool script window (the body of its GUI). You identify widgets on the target application using one of several Learn Tool widgets that are detailed in the following tables. Each use of a scripting widget inserts a script command.  
When executing PuTTY using its GUI, the simplest procedure might be to specify a target address, then execute a connection using PuTTY default parameters. Then automatically submit the username and password to affect a login: First, identify for the Learn Tool the location of the PuTTY Session screen, **Host Name (or IP address)** field. When the script is run, PAM knows where to insert that address.
6. To create the script command that provides this functionality, select the "Text input" tool. Like each of the other Learn Tool scripting controls, this tool invokes an **Add Edit Tag** dialog window. Specify parameters to identify and populate this command in this window.  
The first field is the **Element type**. In this case, select the default "Text Field", which is the type of control widget that PuTTY **Host Name (or IP address)** is. (The other choices are "Drop Down List", "Checkbox", "Radio Button", and "Keystrokes"). To identify where this field is, provide the **Element ID**. The first step is to invoke the application Autolt Control Viewer (v. 1.1) from the Learn Tool menu:

7. Select the "Run Control Viewer" button from the Learn Tool menu bar. You might briefly see a script window, and then in a minute or so the **Control Viewer** window appears. Now you have three windows. The Learn Tool window is resizable.
8. In the Control Viewer window, press and hold your mouse over the **Browse Tool** square area to the upper right. A magnifying glass icon appears, which is your control selection cursor.  
While you hold your mouse down, move this cursor over to the location of the widget (GUI field, or control) that you want to identify.  
As you move the cursor, the control of the target application that is under the cursor displays a red outline. Depending on how the application (PuTTY) was designed, the red outline might refer to a single control or a group of controls.
  - a. If the *specific* control (here, the host name field) is already outlined in red, you would now skip the remainder of this step 10.
  - b. However, a group of controls is selected, and you have not yet been able to identify the **Host Name (or IP address)** field itself.
    - a. Look at the additional characteristics for this specific control that is highlighted in the blue item in the **Controls** list at the bottom of the Control Viewer window. This list also identifies any subordinate controls that are contained by that control. In this case, we want to identify the specific host name control.
    - b. Scroll that list to select the other controls in the list, one by one, until you match the one you are searching for. When the selected control is outlined, note (under the **Control** tab in the central **Info** group) what its full **Instance** name (5) is: here, "[CLASS:Edit; INSTANCE:1]".
9. You have now identified the exact field that PAM must populate. Finish using the Learn Tool **Add Edit Tag** window that you opened in step 8:
  - a. Select the entire **Instance** name (from open bracket to close bracket, inclusive), and copy it in the **Element Id** field.
  - b. In the **Value type** field, select the "text" option. The other two options are "username" and "password." These options refer to data that is supplied by PAM during execution, and not embedded in the script.
  - c. In the **Value** field, enter the IP address that you use to populate that PuTTY field. Alternatively, you can specify a variable hostname by using **\*Value type="host"** (which has a fixed **Value="true"**). In that case, the Device that is associated with the secondary Target Account that is specified in policy is used. See also **Element type='Keystrokes'** in step 14, in which a Target Account is also used to populate the username and password.
  - d. Select **OK** to insert the populated script command. The command appears in the script body. Alternatively, you can specify a variable hostname by using **\*Value type="host"** (which has a fixed **Value="true"**). In that case, the Device that is associated with the secondary Target Account that is specified in policy is used. See also **Element type='Keystrokes'** in step 14, in which a Target Account is also used to populate the username and password.
10. The second element in the PuTTY Configuration window you identify is the **Open** button (on the same screen), which is used to execute the connection:
  - a. Use the Control Viewer procedure of step 10 to identify the **Element ID** for this button.
  - b. Once you have that ID, open the "Mouse click" tool because that is how this PuTTY control is used. The **Add Mouse Click Tag** popup window appears.
  - c. We are using the first option, **Click on the element**. The other option allows you to specify a specific pixel location for the mouse click. Enter the Element ID value that you identified in step 12a into the **ID** field.
  - d. Select **OK** to insert the populated script command. The command appears underneath the first command that you entered.

You have now specified the two elements that provide PuTTY a destination.  
However, the point of the transparent login feature is to insert PAM-supplied credentials transparently. Although the PuTTY application closes its configuration window and opens a console to execute the SSH connection, create a script to provide those credentials. Select the "Save configuration" button to save the current configuration. Then, select the "Add new configuration" button to create another configuration for PuTTY login credentials.  
PuTTY opens its console and communicates with the target Linux Device. Doing this might take some time, and we can account for it in the script.
11. Select the "Sleep" clock icon to open a new widget in which you enter a number of milliseconds. As a rough estimate, you might provide 1000, which allows PuTTY to open and close its windows and be ready with the prompt it receives from its target device.

Now you can assume that your console window is ready with the first of its login prompts from the target, for the username. The Learn Tool allows you to enter a script command that recognizes the Target Account Name:

12. Select the "Text input" again. Set up the **Add Edit Tag** as shown, with **Element type**="Keystrokes" (and then **Element ID**="window" by default) and **Value type**="username".  
Select **OK**. The script command that is created grabs the Account Name from the Target Account that is provided by PAM through your Policy specification. The command then passes it along to the PuTTY target.
13. However, to *submit* the username to the OS then, you have to send a return command. That is, the **Enter** key: Use the "Text input" tool as in the previous step. This time set **Value type**="text", and for **Value**, click your mouse inside its field and press the **Enter** key. The field then displays the text {ENTER} . Select **OK** to insert this tag.
14. Likewise, use the "Text input" tool to set a second command with **Value type**="password". Remember before entering that command to insert another "wait" command using the "Sleep" tool as already explained. You might need to experiment for the most efficient wait times.  
Save this TLC by selecting the (now-active) **Save configuration** floppy disk icon near the right side.  
Now you are ready with your script. However, you might want first to test it to see that it performs as expected. PAM provides this capability with the "Debug" tool.
15. (Optional) To test your configuration, run the Debug tool. This feature executes the currently staged TLC script while displaying debug-level messages in a console.
  - a. Select the "Debug" tool button to open the **Run dialog** window.
  - b. In the **App path** field, use the browse [...] button to the right to specify the location of the RDP Application executable.
  - c. Enter the **Title** of the first window, so that Debug can locate it.
  - d. When credentials and destination must be supplied to execute script processing fully, enter them in **Username**, **Password**, and **Host**.
  - e. When you are ready to run the debug program, select **Run**.  
The Debug console appears.
    - The Debug program first checks each tag for syntax errors, providing feedback in the console, under an initial "App #1" line label.
    - When you bring the RDP Application window (manually) into focus, the Debug program then executes the script. The sequence is labeled ("Try #1"), and then feedback is provided for each tag. If a tag fails to execute successfully, the script is restarted and executes again.
16. (Optional) To improve security in confirming your target application, generate, and copy the SHA-1 digest for the RDP Application. Use the Learn Tool's **Get Application Fingerprint** feature. When configuring the RDP Application in PAM, copy this value into the **Application Fingerprint** field.
17. Continue with [Configure RDP Application](#).

## Reference

The following tables describe the Learn Tool features.

### Learn Tool: Menu Bar

Menu		Description
View	Always on Top	When selected, this feature keeps the Learn Tool window in front of all other windows, even when it is not in focus. The selection state is persistent: After logging off this Device and then logging in again, the option value (whether selected or unselected) remains the same. Default: Selected

Action	Clear cache	Select to remove currently cached applications. When cache is set to "Enable" in <b>Global Settings, Applet Customization, Transparent Login Cache</b> , the Windows target caches the Transparent Login Agent (TLA), Learn Tool, and Control Viewer that are downloaded during connection from PAM when transparent login has been configured, provisioned, and activated. On subsequent connections to that Windows target, the load times for these applications are reduced.
Help	Learn Tool Help	Opens the Compiled HTML (CHM) Learn Tool Help file, which contains detailed descriptions of the Learn Tool controls.
	About	Identifies the Learn Tool application and build versions in a dialog window.

### Learn Tool: XML Scripting Controls

Icon and Tooltip		Description
		One set of <window></window> tags brackets a single-level sequence of XML commands for PAM to manipulate the windows of an RDP Application. Each script control inserts a line containing one XML tag with attributes at the end of the sequence, above the </window> tag. You can copy-and-paste the XML tag lines as in a text editing program, so you can move the lines when and where needed.



Camera icon	Screen verification	<p>Allows insertion of a tag that verifies that a portion of the screen image of the transparent login application matches a previously saved screen capture.</p> <p><b>Usage</b></p> <ol style="list-style-type: none"> <li>1. After selection, the mouse cursor becomes a crosshair, while the full screen area of the RDP window dims and becomes an active grid. Meanwhile, the Learn Tool window is hidden from the desktop so that it does not interfere with screen capture.</li> <li>2. Use the cross-hair cursor to define a rectangle indicating a portion of the RDP Application GUI to be compared to the same GUI during runtime.</li> <li>3. After mouse-up from the cursor, the dialog window Screen Capture Preview displays the comparison Screen capture and the Generated XML Tag to be inserted as PNG.</li> <li>4. Select OK to insert this tag and show the Learn Tool window again.</li> </ol> <p><b>Note:</b> Verify that the captured image portion does not vary from application invocation to invocation, and matches whether the window is active or inactive.</p>
		<p><b>Example:</b> (truncated): &lt;checking content="iVBORu... C6kYII=" /&gt;</p>
Clock icon	Sleep	<p>Allows insertion of a tag that pauses the script for a configurable number of milliseconds.</p> <p><b>Usage:</b> Upon selection, opens the Add Sleep Time Tag pop-up window to specify the milliseconds, then inserts the tag at the end of the script.</p>
		<p><b>Example:</b> &lt;sleep time="500" /&gt;</p>
Keyboard void icon	Freeze Input	<p>Allows insertion of a tag that disables user input (keyboard and mouse events) while a Transparent Login script is running. Freeze Input can prevent re-injection of the user password when using multiple browser tabs. This example freezes user input for 10 seconds. <b>Note:</b> Place this statement at the beginning of your script.</p>
		<p><b>Example:</b> &lt;inputfreeze action="enable"/&gt; &lt;sleep time="10000"/&gt; &lt;inputfreeze action="disable"/&gt;</p>
Duplicate windows icon	Activate window	<p>Allows insertion of a tag that places the named window into focus.</p> <p><b>Usage:</b> Upon selection, inserts this tag at the end of the script.</p>



		<b>Example:</b> <activate />
Mouse icon	Mouse click	Allows insertion of a <click> tag, which affects a mouse-click at a specified location: on a specified button as identified using the Control Viewer; or at the center of the target window; or at a location specified "x" pixels from the left and "y" pixels from the top of the target window.
		<b>Example:</b> button: <click id="[CLASS:Tedit; INSTANCE:2]" /> <b>Example:</b> window center: <click pos="center" /> <b>Example:</b> location: <click x="123" y="72" />

Icon and Tooltip		Description
Page with pencil	Text input	Allows insertion of a tag that submits one of these data types: <ul style="list-style-type: none"> <li>Edits a specified control (field, drop-down list, checkbox, radio button) so that it contains specified data (text, sequence value, Boolean value).</li> <li>Sends a text string, which is composed of literal values, key stroke shortcuts or labels, or parameters provided by PAM such as username or password.</li> </ul>

		Element type	Element ID	Value type	Value
		"Text Field"	as determined through the Control Viewer – see the example in the procedure.	"text"	String, to populate the field
				"username", or "password", or "host"	"true": For the specified Value Type, TLA sends the Value that is attached to the user policy through the target account record.
		"Combobox"		"text"	String, matching a (drop-down) list option
				"index"	Integer, as specified to select the ordinal location of a (drop-down) list option

		"Keystrokes"	"window" (or none)	"text"	As specified: (a) strings, and (b) key stroke tags: (i) entered into the dialog field by typing merely the named key: • includes: .ENTER,ESCAPE, TAB. • appear as: {ENTER}, {ESCAPE}, {TAB} • only one is permitted per XML tag. (ii) entered by typing the key sequence: for example: {F1} entered by typing the four keys: .{+ .F + 1 +} +
				"username", or "password", or "host"	"true": For the specified Value Type, TLA sends the Value in the Target Account that is chosen for the RDP Application that is specified in the PAM policy.
		<b>Element type</b>	<b>Element ID</b>		<b>Checked</b>
		"Checkbox"	As determined through the Control Viewer	"True" or "False"	
		"Radio Button"	"True"		

		<b>Example:</b> (using "Text Field", "text" options in dialog): The following tag inserts the text string "123" (without quotes) into the ID-specified text field: <edit id="[CLASS:TEdit; INSTANCE:1]" text="123" />
Checkmark icon	Element Verification	Allows insertion of a tag that confirms or denies the existence of an element. Optionally verifies that element in a specified state (for example, a text field containing a particular string).
		<b>Element types:</b> Text field   Combobox   Checkbox   Radio Button <b>Element ID:</b> Code identification of the GUI feature that is obtained through Control Viewer. <b>Value:</b> Literal. Ranges: Checkbox and Radio Button: (only) "checked" <b>Example:</b> The following tag verifies that the radio button that is identified has been selected: <verify component="radiobutton" id="[CLASS:TRadioButton; INSTANCE:3]" /> If the component is not confirmed, the TLC script halts.

**Learn Tool: Utilities**

Icon and Tooltip		Description
Page with magnifying glass	Run Control Viewer	<p>Runs the third-party, Learn Tool bundled application, Autolt Control Viewer version 1.1.</p> <p>This application can be used to determine the Element ID when needed in a script command. (No other Control Viewer functions are needed for PAM use.)</p> <p><b>Usage:</b> (to identify a control or widget): See example in steps 9-10 of the procedure.</p> <p><b>Usage:</b> (to identify a window name): To populate the &lt;window id= ""&gt; XML tag (top line of the TLC):</p> <ol style="list-style-type: none"> <li>1. From the Control Viewer window in the Browse Toolbox in the upper right, click your mouse button and hold it down to show the magnifying glass cursor.</li> <li>2. While holding your mouse button down, drag the cursor so that it is over your RDP Application window title bar, then release your mouse button.</li> <li>3. In the <b>Control Viewer Info</b> panel, <b>Window</b> tab, <b>Class</b> row, copy the text from its field. For example, for PuTTY, Control Viewer might display "PuTTYConfigBox".</li> <li>4. Paste the text from that field into the following string: [CLASS:WindowID; INSTANCE:1] substituting "WindowID" with your actual value.</li> <li>5. Paste the entire revised string between the quotation marks into the &lt;window id="" /&gt; tag on the first line of your TLC.</li> </ol> <p><b>Example:</b> &lt;window id="[CLASS:PuTTYConfigBox; INSTANCE:1]" /&gt;</p>

Fingerprint	Get Application Fingerprint	<p>Calculates and displays an application fingerprint for an RDP Application so that it can be used during transparent login attempts.</p> <p><b>Usage</b></p> <ol style="list-style-type: none"> <li>1. Select this button to open the Get Application Fingerprint dialog window. Select the path location of the application executable and a fingerprint string is generated and populated into the Application Fingerprint field. Copy the full text string into the Ctrl-C buffer or a text file.</li> <li>2. Paste the fingerprint to the corresponding Application Fingerprint field of a PAM RDP Application record.</li> <li>3. When PAM makes a transparent login attempt, it first checks this stored fingerprint against one generated for the RDP Application that is discovered on the target RDP server (Windows Device). If the fingerprints do not match, the attempt is canceled.</li> </ol>
Play icon	Debug	<p>Runs the TLC script currently staged in the Transparent Login Configuration panel (the main body of the window).</p> <p><b>Usage:</b> See the example in Step 17 of the previous procedure.</p>

### Learn Tool: File Controls

Icon and Tooltip		Description
Drop-down list	Filter by name / (configuration name)	Displays the name of the configuration staged in the Transparent Login Configuration field (the 'body' of the window).

	(configuration list)	<p>This drop-down list lists transparent login configurations, either:</p> <ul style="list-style-type: none"> <li>(a) all staged in the Learn Tool</li> <li>(b) filtered by name (string) entered</li> </ul> <p>When the Learn Tool is launched following an RDP connection, these configurations are copied from the full set that is managed in PAM Services, RDP Applications, Transparent Login Configurations. The initial set of configurations can include several configuration samples (for example, for PuTTY or WinSCP) corresponding to recent versions of those applications.</p>
Page with plus sign	Add new configuration	<ol style="list-style-type: none"> <li>1. Opens a dialog window into which you can enter the name for a new configuration.</li> <li>2. Upon selecting OK, the Learn Tool body is cleared (to &lt;window&gt; tags), a new config file is created on PAM with that name, and the name is loaded into the drop-down field.</li> <li>3. Upon creation of new XML tags, the name is marked with a preceding asterisk, indicating unsaved changes.</li> </ol>
Duplicate pages	Copy configuration	<ol style="list-style-type: none"> <li>1. While a configuration file is staged, this button opens a dialog window into which you can enter the name for a new configuration.</li> <li>2. The content of the first configuration is then copied into the new configuration so it appears in the Learn Tool GUI as if only the name has changed. You can then edit and save to that new file.</li> </ol>
Page with X	Remove configuration	<ol style="list-style-type: none"> <li>1. Opens a dialog window for confirmation.</li> <li>2. Upon selection, removes the currently staged configuration from the Learn Tool and from the file from PAM.</li> </ol>
Inactive - gray floppy disk Active - blue floppy disks	Save configuration	When active, saves the currently displayed configuration to PAM.
Inactive - gray floppy disks Active - blue floppy disks	Save all changes	When active, saves all configurations that are staged in the Learn Tool drop-down (that differ from currently saved versions) to PAM.
Cycle arrow	Refresh all	Loads all currently saved PAM TLCs into Learn Tool. If there are unsaved configurations in the Learn Tool, they are erased.

## Configure an RDP Application

After using Learn Mode, you have a transparent login configuration in PAM that you can apply to the RDP Application you are targeting.

### Follow these steps:

1. Navigate to **Services, Transparent Login Configurations**.  
Here you can confirm that the configuration you created with the Learn Tool is now available for use.
2. Select the line item for your configuration, and confirm that it is as created in the Learn Tool.  
Alternatively, you can create a configuration file from scratch by selecting the **Add** button to open a blank template and populate it. Configuration files are not dependent on creation with the Learn Tool.
3. Return to **Services, Manage RDP Applications**.
4. Select the **Add** button to open a blank template.
5. Enter an **RDP App Name** that is helpful to users when they access the link from their Access pages.
6. In **Launch Path**, provide the Windows pathname for the local target drive location of the application.
7. (Optional) - Select **Hide From User**. Select this option if you want a user to access the RDP applications in an RDP access method, but not allow the user individual access to the RDP application.
8. On the **Transparent Login** tab, select the **Transparent Login** box.
9. (Optional) In the **Application Fingerprint** field, paste the SHA-1 digest you generated while using the Learn Tool.
10. Select **OK**. A new line identifies the window of this RDP Application that is used to execute a transparent login. After PAM identifies the title of the designated window, it executes the associated configuration to perform transparent login, or other behavior requiring credentials supplied by PAM.
  - a. Enter the **Window Title** that is displayed in the RDP Application GUI.
  - b. From a drop-down list of currently managed transparent login configuration files (see Step 2), select an appropriate configuration in the **Transparent Login Configuration** field.
  - c. If you want this configuration to be available to the user during any RDP session (with access to the Windows Desktop) to this target Device, and not exclusively during a session to this RDP Application, set the **RDP Session** option. When the user connects to an RDP server, the Transparent Login agent is loaded and runs in the background. Once the configured RDP Application is launched, the Transparent Login Agent detects it and automatically fills out the necessary information to proceed. Enable this option if you are using **Hide From User** in step 7.
  - d. If you want to assign more transparent login configurations using this RDP Application, create more line items using **Add Window**. (For example, using PuTTY, you might specify alternate targets or a different login parameter.)
11. Select **Save**.
12. Edit the PAM Device record for the Windows RDP server so that it uses this RDP Application, now listed under **Services**.

## Activate the Policy

When you associate a Transparent Login RDP Application Service with a PAM policy, specify target accounts for use by the Transparent Login Agent on the target device. These target accounts are referred to as Transparent Login Credentials. They are the credentials that are used to fill in the "username" and "password" attributes in the Transparent Login scripts that are generated by the Learn Tool. They are associated with the Transparent RDP application.

### Follow these steps:

1. Ensure that the Transparent Login RDP Application is associated with the correct Target Device. Follow the steps to associate a Service with a Device.
2. Navigate to **Policies, Manage Policies**. Select the **Add** button to create a new policy or **Update** to add the Transparent Login RDP Application service to an existing policy.
3. Select the **Enabled** checkbox on the **Transparent login** tab to enable Transparent Login for this policy.

4. Select the **Services** tab.
5. Locate the Transparent Login RDP Application Service under **Available Services** and select the service. Use the right-arrow icon to move the service to the **Selected Services** area.
6. Select the login target account for auto login into the policy device. Select the gray magnifying glass icon under the **Target Account** column.
7. When you select a Transparent Login RDP Application service, the bottom half of the tab populates with the details about the service. If you do not require Transparent Login Credentials for the service, select **OK** to save the policy.
8. Select the magnifying glass icon next to **Transparent Login Credentials** on the bottom right of the tab.
9. Select the accounts that you want to make available for use with the selected Transparent Login RDP Application Service and select **OK**. These are the accounts that the Transparent Login Agent offers for use when the end user accesses a Transparent Login application from the **Access** panel.

#### **IMPORTANT**

To insert account credentials transparently, the Transparent Login Agent must be able to retrieve the password for the selected target account without further user interaction. The **Reason Required for Auto Connect** option must therefore be disabled in the [password view policy](#) associated with each target account.

### **Caching**

Depending on your security needs, and after using the Learn Tool and testing transparent login configurations, you might enable the Transparent Login Cache. This feature caches the Learn Tool (when used), the Transparent Login Agent, and the Control Viewer (when Learn Tool is used) on the RDP server. They do not need to be loaded onto a temporary local drive during each login at that Device, thus reducing application startup time.

### **Configuration**

To turn on caching, set **Global Settings, Applet Customization, Transparent Login Cache** = "Enable" .

### **Usage**

During login at a particular target, you see confirmation of the caching storage in the RDP initialization console of each application cached.

### **Auditing**

You can use logs and session recording for auditing access attempts.

- Logs  
PAM logs each access attempt, for example:

```
2016-03-11 01:16:27 super login Win 2008 R2 (32-bit) Xsuite user transparently logged
into RDP Application "putty.exe" to "PuTTY Configuration" window as "dev"
```

- Session Recording  
A session recording marks the location of the secondary transparent login attempt. For RDP connections to Windows, these attempts are marked in the **Events** list and by a red arrow on the timeline. You can see event detail as a tooltip from the line item in the **Events** list, and in the **Info** box at the lower left and in a pop-up window during cross-over on the timeline.  
For transparent login activity to be successfully recorded when the user has Internet Explorer, the administrator must configure all equivalent PAM addresses. Example: A cluster VIP name and VIP address in the browser security settings. See [Set Up Session Recording](#).

### **User Experience**

Script windows and the application interface are displayed briefly as the automation proceeds, and stops showing changes when the script completes.

Following selection of the RDP Application link PuTTY, the user sees this sequence following login at the RDP server host:

1. The console for the RDP session initialization appears.
2. The console for the transparent login Agent (TLA) that is running on the local virtual drive appears.
3. The RDP Application (PuTTY) is invoked, and (in this case) a configuration GUI is auto-populated and activated by the transparent login script, eventually invoking a second interface (the PuTTY console).
4. The RDP Application (PuTTY) invokes a new window (the console interface), and is auto-populated by the continuing transparent login script. After the script completes, the console interface is ready for user access.

## Import or Export Transparent Login Configurations

1. Select **Services, Transparent Login Configurations**.
2. Click the **Import/Export** button.  
The Import/Export window appears.
3. Click **Download Sample File** to save a template file to a convenient editing location.
4. Copy the sample to a new file, and open it in a spreadsheet program or a plain-text editor.
5. Edit or add line items for each configuration and save the file. For descriptions of each field, see [CSV File Format](#).

### NOTE

Do not alter the first (header) line.

6. Click **Choose File** to browse for your saved CSV file.
7. Click **Import Transparent Login Configurations**.

### CSV File Format

- To handle dependencies, when provisioning multiple objects using CSV files, Transparent Login Configurations should be the last group imported. Ensure that any related Services, Roles, User Groups, Users, Device Groups, Devices, Socket Filter Lists, Command Filter Lists, and Policies are configured first.
- Commas are the only allowed field separators, so a comma cannot be used in any field content.
- The first line in the file is for column names and is used for categorization during import.
- The Transparent Login Configurations CSV file has only three columns, all required:
  - **Type:** The only type that is allowed is "SSO Config".
  - **Name:** Enter a string, such as "Putty".
  - **Configuration:** Enter an XML single-level structure that is bounded by window tags. This XML script is applied to the application during transparent login use. For example:

```
<window> <activate/> <combobox id="[CLASS:Edit; INSTANCE:1]" index="1"/> </window>
```

### Export a CSV File

To export a CSV file of you existing Transparent Login Configurations, follow these steps:

1. Select **Services, Transparent Login Configurations**.
2. Click the **Import/Export** button.  
The Import/Export window appears.
3. Click the **Export Transparent Login Configurations** button to export a CSV file.

## Configure Support for Citrix Virtual Apps Resources

You can configure Privileged Access Manager to support the following specific resource types in a Citrix Virtual Apps environment:



- **Citrix StoreFront:** Access, transparent (automatic) login, and session recording.
- **Citrix XenDesktop:** Direct access, transparent (automatic) login, and session recording.

**Published Virtual Apps applications:** Direct access and session recording.

#### NOTE

Transparent login is not currently supported for published Citrix Virtual Apps applications.

This topic has the following contents:

### Requirements

Verify that the following requirements are configured in your Citrix Virtual Apps environment:

- HTML5 client is enabled on the Citrix Workspace.
- WebSocket connections are enabled on Citrix Virtual Apps and Citrix Virtual Apps and Desktops.
- If Privileged Access Manager and Citrix Virtual Apps are in different subnets, configure Citrix Workspace to allow remote users to access stores through NetScaler Gateway using the Enable Remote Connections task. For more information, see the Citrix Virtual Apps documentation for your version of Workspace.
- By default, concurrent connections by the same user from different IP addresses are not allowed. Because there are use cases where this concurrence might be necessary, there is an option to allow it. For example, your Citrix Virtual Apps environment might have several jump boxes and a load balancer. An end user might run several sessions simultaneously, and the user sessions originate at different jump boxes. If this concurrence is necessary, you can allow concurrent connections. Select **Enabled** for **Concurrent Remote Connections Allowed** on the **Configuration, Security, Access** Page. By default, this setting is set to **Disabled**.

### Configure a Service for Citrix Workspace

Use this procedure to configure a service for Citrix Workspace.

#### Follow these steps:

1. From the Menu bar, select **Services, Manage TCP/UDP Services**.
2. Select **Add**.
3. Complete the following fields:
  - **Service Name:** A unique name, for example, "Virtual\_Apps\_All".
  - **Ports:** *Workspace\_Ports*  
Where *Workspace\_Ports* are the port numbers for Workspace, separated by a colon. For example, "80:6513".
  - **Application Protocol:** Web Portal
  - **Launch URL:** https://<Local IP>:<First Port>/<Path\_to\_Workspace>  
Where *Path\_to\_Workspace* is the browser path to Workspace. For example, "Citrix/Store1Web"
  - **Browser Type:** PAM Browser
  - **Auto-Login Method:** PAM HTML Web SSO  
(Accept the default values for other fields.)
4. Select **Save**.

### Configure a Service for XenDesktop

Use this procedure to configure a service for Citrix XenDesktop.

#### Follow these steps:

1. From the Menu bar, select **Services, Manage TCP/UDP Services**.
2. Select **Add**.
3. Complete the following fields:

- **Service Name:** A unique name, for example, "Virtual Apps\_Desktop."
  - **Ports:** *XenDesktop\_Ports*  
Where *XenDesktop\_Ports* are the port numbers for XenDesktop, separated by a colon. For example, "80:6611"
  - **Application Protocol:** Web Portal
  - **Launch URL:** https://<Local IP>:<First Port>/<Path\_to\_XenDesktop>  
Where *Path\_to\_XenDesktop* is the browser path to XenDesktop. For example, "Citrix/Store2Web"
  - **Browser Type:** PAM Browser
  - **Auto-Login Method:** PAM HTML Web SSO  
(Accept the default values for other fields.)
4. Select **Save**.
  5. In the StoreFront console, navigate to **Stores, XenDesktop\_Store, Manage Receiver for Web Sites, Configure, Client Interface Settings**. Verify that the **Auto launch desktop** option is set.

### Configure a Service for Virtual Apps Applications

Use this procedure to configure a service for your Citrix Virtual Apps applications.

#### **Follow these steps:**

1. From the Menu bar, select **Services, Manage TCP/UDP Services**.
2. Select **ADD**.
3. Complete the following fields:
  - **Service Name:** A unique name, for example, "Virtual Apps\_Apps."
  - **Ports:** *Virtual Apps\_App\_Ports*  
Where *Virtual Apps\_App\_Ports* are the port numbers for your Virtual Apps applications, which are separated by a colon. For example, "80:6813"
  - **Application Protocol:** Web Portal
  - **Launch URL:** https://<Local IP>:<First Port>/<Path\_to\_Virtual Apps\_Apps>  
Where *Path\_to\_Virtual Apps\_Apps* is the browser path to your Virtual Apps applications. For example, "Citrix/Store3Web"
  - **Browser Type:** PAM Browser
  - **Auto-Login Method:** PAM HTML Web SSO  
(Accept the default values for other fields.)
4. Select **Save**.
5. In the StoreFront console, navigate to **Stores, Virtual Apps\_App\_Store, Manage Receiver for Web Sites, Configure, Client Interface Settings** and set the **Auto launch desktop** setting.

### Configure a Device for Virtual Apps

Use this procedure to configure a device for Virtual Apps.

#### **Follow these steps:**

1. From the Menu bar, select **Devices, Manage Devices**.
2. Select **ADD**.
3. Complete the following fields:
  - **Name:** A unique name, for example, "Virtual Apps"
  - **Address:** The IP address of the Virtual Apps server.
  - **Device Type:** Select the following option: **Access**. Optionally, select **Password Management**.
  - **Services:** Select **Add** and select the services that you configured for Virtual Apps resources. In this example, **Virtual Apps\_All, Virtual Apps\_Desktop, and Virtual Apps\_Apps**.  
(Accept the default values for other fields.)

4. Select **Save**.

### **Configure a Policy for Your Virtual Apps Resources.**

Configure a policy to associate your Virtual Apps device and its services with users who require access. If session recording is required, select **Web Portal** from the **Recording** options.

#### **NOTE**

Multiple users can launch CA PAM Client instances from *different* Virtual Apps sessions. That is, each user must start their own Virtual Apps session because multiple user logins from a *single* Virtual Apps session do not guarantee attribution and confidentiality.

## **Configure Users**

Each person accessing resources through PAM must have a user account.

A **user** represents a login account with a specific set of privileges to perform actions on the appliance. Every login account constitutes a user. Users are displayed, defined, and managed through the **Users** menu in the UI.

#### **NOTE**

When referring to users managed by the appliance, the user is a managed object or account. This user is distinct from the actual person ("user") who uses the managed account.

### **Privileges and Roles**

Each user must be represented by at least one **role** attribute. A role is a set of access privileges. Each privilege allows the user to perform certain functions on the appliance.

A set of predefined roles is provided with the basic installation. These user types include:

- **End Users**

An end user is a managed user who primarily accesses managed devices and views a password of a managed target account. This user has a predefined role of Standard User, which is assigned by default when the User template is used to create an account. All end-user activity is performed on the Access page (which is unlabeled). These Users have no access to the Admin menu.

#### **NOTE**

The privileges of a Standard User are *not* a subset of all other predefined roles. There are administrator roles that do not allow access or password viewing.

- **Administrators**

An **administrator** is a user who can exercise privileges beyond Standard User privileges. As a result, an administrator sees a full or partial Admin menu, or has access to the Config menu.

- **super and config administrators**

Two administrator accounts, **config** and **super**, are predefined on the appliance. These two administrators have certain special privileges and characteristics to perform initial configuration and other operations:

- **super** has a predefined role of Global Administrator. This role appears in the Users list on the Manage Users page.
- **config** has access only to the Configuration menu, including the Change Password menu. The config user does not appear on the Users list on the Manage Users page.

The privileges of the config account differ from the privileges that are assigned to the Configuration Administrator role. The config user gains access solely through the /config/ directory. The config user is also the only account with access to the Change Password menu.

Though you can change the names of the super and config users, we recommend that you leave the names as is. If you do change the names, these two accounts always constitute the two baseline user accounts.

## User Groups

**User Groups** let you apply user attributes to all members belonging to a group.

### NOTE

Privileged Access Manager user groups are distinct from Credential Manager user groups.

## Configuring User Accounts

User accounts can be created in two ways:

- Individually using the UI
- Imported from a CSV file, which contains a set of user records. When users are imported from a CSV file, these users are automatically established as a group.

## More Information

For more information, see the following articles:

- [User Roles](#)
- [Identify User Roles and Privileges](#)
- [Identify Users that Can Log in to the Server](#)
- [Configure User Groups](#)
- [User / User Group Management](#)
- [User Viewing](#)

## User Roles

To perform operations in Privileged Access Manager, each user must be assigned one or more *user roles*, which define sets of privileges that are related to different product functions. The many available [predefined roles](#) should satisfy most requirements. By default, new users are assigned the *Standard User* role, which allows them to access devices. Assign roles with more privileges to administrators. You can also create custom roles to assign privileges to match your own requirements. You manage roles from the **Users, Roles** screen.

## Manage Credentials Privilege

This content covers user roles for provisioning privileged access to devices and applications. For information about Credential Manager roles, see [Add or Modify Credential Manager Roles](#). However, users who require Credential Manager administrative privileges must be assigned a user role with the *Manage Credentials* privilege. The following preconfigured user roles provide the Manage Credentials privilege:

- Global Administrator
- Operational Administrator
- Password Manager

Also, by default, users are assigned to the "[Standard User](#)" role and are *silently* assigned to the "Standard Users" Credential Manager group. ("Standard Users" is not shown on the **Credential Manager Groups** tab). Membership of the "Standard Users" Credential Manager group provides privileges to view account passwords on the **Access** page. However, when a user is assigned any role with the "Manage Credentials" privilege (for example, "Password Manager"), that user is removed from the "Standard Users" Credential Manager group and cannot view passwords on the **Access** page. To find out how to provide password viewing privileges, see [Configure Users with the Manage Credentials Privilege to View Passwords on the Access Screen](#). To learn how to view the Target Account's password credential history, see [Configure a PAM User to View the Password History of Target Accounts](#).

**NOTE**

If you are creating a custom role that need to manage the Credential Manager's "System Admin Group", then add the Global Administrator role to the custom role.

**Identify User Roles and Privileges**

Privileged Access Manager provides a preconfigured set of user roles. You can also configure your own roles from a set of available user privileges.

**Predefined Roles**

A predefined set of roles is provided with the product. View these roles by selecting **Users, Manage Roles**. This set has the privileges that are required to perform various common activities. Roles are assigned to Users and User Groups during their creation and editing. See [Configure Users](#) for more information.

The following table lists the predefined roles:

Role	Description	Privileges
Administrative Auditor	Allow user read only access to administrative pages (services, users, devices, policies).	Read Services, Read Users, Read User Groups, Read Socket Filter Agent, Read Devices, Read Device Groups, Read Policies, Read Socket Filters, Read Command Filters, Read Roles
Auditor	Allow users to view PAM logging, session recording, and reporting data. Auditors have read-only access to Global Settings to inspect settings that have impact on log data.	Read Overview, All Logging, Read Session Recordings, Read Global Settings
Autodiscovery	Allow users to use the autodiscovery feature to find network devices.	autodiscovery
AWS API Proxy User	Allow the user to log in, select the access page, and remotely access the AWS API Proxy.	Access All, AWS API Proxy, Manage All
CA TAP API User	All the privileges that are needed for CA Threat Analytics to use the external API.	Access All, Manage BAP API, Read Devices, Read Users, Manage Sessions
Configuration Manager	Allow users to set "Global Settings" and access all "Configuration" tabs.	Read Global Settings, Manage Global Settings, Manage Configuration
Delegated Administrator	A combined user role that grants to users the ability to perform all User, Device, and Policy Manager tasks.	Read Users, Manage Users, Delete Users, Assign Users, Read User Groups, Upgrade User Groups, Approve CAC User, Read Socket Filter Agent, Delete Socket Filter Agent, Read Devices, Manage Devices, Delete Devices, Assign Devices, Read Device Groups, Update Device Group, Read Policies, Manage Policy, Read Socket Filters, Manage Socket Filters, Read Command Filters, Manage Command Filters, Manage User RDP User Name
Device and Device Group Manager	Allow users to read, create, update, and delete all types of devices.	Read Socket Filter Agent, Delete Socket Filter Agent, Read Devices, Manage Devices, Delete Devices, Assign Devices, Read Device Groups, Update Device Group

Global Administrator	Allow access to all and configuration of all Privileged Access Manager functionality.	Access All, Manage All, Monitor All, Read Sessions, Manage Sessions, Read Overview, All Tools, All Logging, Read Session Recordings, Read Global Settings, Manage Global Settings, Read Services, Manage Services, Delete Services, Read Users, Manage Users, Delete Users, Assign Users, Read User Groups, Upgrade User Groups, Approve CAC User, Read Socket Filter Agent, Delete Socket Filter Agent, Read Devices, Manage Devices, Delete Devices, Assign Devices, Read Device Groups, Update Device Group, Read Policies, Manage Policy, Read Socket Filters, Manage Socket Filters, Read Command Filters, Manage Command Filters, Import Policy, Export Policy, Manage Configuration, Read Roles, autodiscovery, Manage Credentials, Manage User RDP User Name Please see <a href="#">this important note</a> about roles with the Manage Credentials privilege.
Global Setter	Allow users to set "Global Settings".	Read Global Settings, Manage Global Settings
Management Console API User	Allow user access to CA Management Console API (Internal use only).	Manage Management Console API
Monitor	Allow users to monitor devices.	Monitor All
Operational Administrator	Allow access to all PAM administrative functionality, without configuration management.	Access All, Manage All, Monitor All, Read Sessions, Manage Sessions, Read Overview, All Tools, All Logging, Read Session Recordings, Read Global Settings, Manage Global Settings, Read Services, Manage Services, Delete Services, Read Users, Manage Users, Delete Users, Assign Users, Read User Groups, Upgrade User Groups, Approve CAC User, Read Socket Filter Agent, Delete Socket Filter Agent, Read Devices, Manage Devices, Delete Devices, Assign Devices, Read Device Groups, Update Device Group, Read Policies, Manage Policy, Read Socket Filters, Manage Socket Filters, Read Command Filters, Manage Command Filters, Import Policy, Export Policy, Read Roles, autodiscovery, Manage Credentials, Manage User RDP User Name Please see <a href="#">this important note</a> about roles with the Manage Credentials privilege.
Password Manager	Allow users to configure Credential Manager.	Manage Credentials Please see <a href="#">this important note</a> about roles with the Manage Credentials privilege.
Policy Manager	Allow users to read, create, update, and delete all policies, socket and command filters, and agents.	Read Socket Filter Agent, Delete Socket Filter Agent, Read Policies, Manage Policy, Read Socket Filters, Manage Socket Filters, Read Command Filters, Manage Command Filters
Secrets Management	Allow users and user groups to access the Secrets Management functionality.	<code>Enable Secrets Management</code> Users with this role are still unable to see or manage any vaults or secrets until they are assigned a Vault Owner, Secrets Owner, or a Secret Viewer role for a vault. See <a href="#">About Secrets Management and Roles</a> for procedures on assigning these more granular roles.

Server Control Administrator	Allow users to access the Server Control and UNAB policy management functionality.	Add Device Group, Delete Device Group, Read Device Group, Update Device Group, Assign Devices, Delete Devices, Manage Devices, Read Devices, All Logging, Read Server Control Deployment Audit Log, Deploy Server Control Policies, Read Device/Device Group Server Control Policy Assignments, Manage Server Control Policies, Read Server Control Policies, Manage UNAB Login and Config Policies, Add User Group, Delete User Group, Read User Groups, Update User Group, Assign Users, Delete Users, Manage Users, Read Users
Server Control Deploy Manager	Allow users to Assign, Unassign, Upgrade, and Downgrade Server Control Policies.	Read Device Group, Read Devices, Read Server Control Deployment Audit Log, Deploy Server Control Policies, Read Device/Device Group Server Control Policy Assignments, Read Server Control Policies
Server Control Policy Editor	Allow users to Create, Copy, Update, and Delete Server Control Policies.	Manage Server Control Policies, Manage User RDP User Name
Service Manager	Allow users to read, create, update, and delete service.	Read Services, Manage Services, Delete Services
Session Manager	Allow users to view and terminate PAM login and remote access.	Read Sessions, Manage Sessions
Standard User	Allow users to access and manage remote devices.	Access All, Manage All, Manage User RDP User Name
Target Connector Validator	Allow users to view and use the Target Connector Framework validator. The validator examines UI definitions from a JSON file, which renders pages for custom target connectors.	Validate Target Connector UI
Troubleshooter	Allow users to access the <b>Configuration, Tools</b> page	All Tools
UNAB Manager	Allows access to UNAB Host Login Policy management and UNAB Configuration Token management on devices and device groups.	Add Device Group, Delete Device Group, Read Device Group, Update Device Group, Assign Devices, Delete Devices, Manage Devices, Read Devices, All Logging, Manage UNAB Login and Config Policies, Add User Group, Delete User Group, Read User Groups, Update User Group, Assign Users, Delete Users, Manage Users, Read Users, Manage User RDP User Name
User and User Group Manager	Allow users to read, create, update, and delete all types of users	Read Users, Manage Users, Delete Users, Assign Users, Read User Groups, Upgrade User Groups, Approve CAC User, Manage User RDP User Name
VMware NSX API Proxy User	Allow the user to log in, select the access page, and remotely access the VMware NSX API Proxy.	Access All, Manage All, VMware NSX API Proxy

### Privilege Definitions

In addition to the set of predefined roles, administrators can also create custom roles. Create a custom role by selecting from a list of available privileges, as shown in the following table.

Role Privilege	Actions Allowed
Standard User	

Access All	Use the access page to connect to remote machines.
Manage All	Use the manage devices page to perform actions like power cycling remote machines.
<b>Monitoring</b>	
Monitor All	Use the monitor page to view the status of remote devices.
<b>Sessions</b>	
Read Sessions	Look at the manage sessions/logins page.
Manage Sessions	Use the manage sessions/logins page to kill sessions and logins.
Read Overview	Examine devices, out of band devices, and connections.
<b>Tools</b>	
All Tools	Use configuration tools such as ping and traceroute.
<b>Logging / Recordings</b>	
All Logging	Look at the log page and execute reports.
Read Session Recordings	Replay session recordings.
<b>Global Settings</b>	
Read Global Settings	See global settings.
Manage Global Settings	Alter global settings.
<b>Services</b>	
Read Services	See details of all services, of any type (TCP, RDP Application).
Manage Services	Add or change any existing services of any type (TCP, RDP Application).
Delete Services	Delete any existing services of any type.
<b>Users</b>	
Read Users	See details of all users. Allows export of users.
Manage Users	Create or change users including export. Allows import of users.
Delete Users	Delete any non-LDAP users.
Assign Users	Assign a user to a user group or a user group to a user.
Read User Groups	See details of user groups.
Upgrade User Groups	Change existing user groups, but not their memberships.
Approve CAC User	Approve candidate CAC users.
Read Roles	Read roles and privilege definitions.
Manage User RDP User Name	Edit the RDP User Name field in a user definition.
<b>Socket Filters</b>	
Read Socket Filter Agent	View socket filter agents.
Delete Socket Filter Agent	Delete socket filter agents.
Read Socket Filters	See socket filter lists and configuration.
Manage Socket Filters	Change or remove socket filter lists and configurations.
<b>Devices</b>	
Read Devices	See details of all devices, including power hosts and consoles. Allows export.
Manage Devices	Create and change devices and their memberships. Allows import.



Delete Devices	Delete any devices.
Assign Devices	Assign a device to a device group or assign a device group to a device.
Read Device Groups	See details of device groups.
Update Device Group	Change existing device groups, but not their memberships.
autodiscovery	Find devices on the network.
<b>Policy</b>	
Read Policies	See policies. Do not allow export.
Manage Policy	Change or remove policies. Do not allow import.
Import Policy	Import all kinds of associations.
Export Policy	Export all kinds of associations.
<b>Command Filters</b>	
Read Command Filters	See command recording lists and configuration.
Manage Command Filters	Change or remove command filter lists and configurations.
<b>Configuration</b>	
Manage Configuration	Use the Access configuration tab.
<b>Passwords</b>	
Manage Credentials	Create and update credential definitions for password chaining.
<b>APIs</b>	
AWS API Proxy	Allow access to the AWS (Amazon Web Services) API Proxy.
Manage BAP API	Manage the CA Threat Analytics API.
managementConsole	Manage the Management Console API.
nsxApiProxy	Allow access to the VMware NSX API Proxy.
<b>Server Control Policies</b>	
Deploy Server Control Policies	Assign, Unassign, Upgrade, and Downgrade Server Control Policies
Manage Server Control Policies	Create, Read, Update, and Delete Server Control Policies
Manage UNAB Login and Config Policies	Read, Write, and Delete UNAB Host Login Policies, as well as UNAB Configuration Token Definitions
Read Device/Device Group Server Control Policy Assignments	Look at Server Control Policy Assignments on Devices/Device Group
Read Server Control Deployment Audit Log	Look at Server Control Deployment Audit Log
Read Server Control Policies	See details for all the Server Control Policies
<b>Secrets Management</b>	
Enable Secrets Management	Allows access to the Secrets Management functionality. Users with this privilege are still unable to see or manage any vaults or secrets until they are assigned a Vault Owner, Secrets Owner, or a Secret Viewer role for a vault. See <a href="#">About Secrets Management and Roles</a> for procedures on assigning these more granular roles.

## User Role Cases

### Expanded User Privilege Assignment Under Restricted Administration

Privileged Access Manager administrators with less than a Global Administrator role were once restricted from creating or updating Users beyond Standard User or Monitor roles. Administrators could not then update their own profile, or that of any other User, with privileges higher than their own. This feature is named "restricted administration."

#### **NOTE**

Earlier implementations of restricted administration have also been known as "delegated administration." However, this feature name can easily be confused with the unrelated Delegated Administrator role. Privileged Access Manager documentation no longer uses the term "delegated administration."

Restricted administration is now fine-tuned to allow full assignment of any set of privileges less than one's own. An administrator below a Global Administrator can assign preset or custom roles other than Standard User or Monitor, up to and including its own privileges. Conversely, restricted administration prevents the assignment of roles, groups, and other objects that overstep the applicable privileges.

#### ***Provisioning Expanded User Privilege Assignment***

Assume that your organization has a population of Devices that are maintained in two geographical or network locations or regions. For each region, you want to assign an administrator with Delegated Administrator privileges to manage only its own Users and Devices. Meanwhile, a User Group is assigned the Device/Group Manager role to manage all Devices in both regions.

The options available to one of these two administrators when creating a User are then restricted. The Delegated Administrator role permits the required privileges within the User/Device scope. The Available Roles for this new User are therefore the "Delegated Administrator", its components ("Device/Group Manager", "Policy Manager", and "User/Group Manager"), and the typical "Standard User" (assuming this administrator also performs Device or credentials access activities).

Meanwhile, the Available Groups list identifies all User Groups that exist on this Privileged Access Manager appliance. The "DeviceManagers" group is dim, which allows management of all Devices rather than only those managed by this administrator. Because its choice would effectively result in elevated privileges, it cannot be selected.

## **Import and Export Roles**

### ***Configure Internet Explorer***

To use the Import/Export functions with Internet Explorer (IE), changes might need to be made to the security settings. To establish IE security settings:

1. Open IE browser.
2. Select **Tools, Internet Options**.
3. In the Internet Options pop-up window, select the **Security** tab.
4. Select the slider zone
5. Select **Custom level**. Scroll to **Downloads**. For **File download**, select the **Enable** option.
6. Select **OK** to save changes.

### ***Import Roles from a CSV***

To import the Roles, follow these steps:

1. Go to **Users, Manage Roles**.
2. Select the **Import/Export** button.  
The Import/Export Roles window appears .
3. Select Download Sample File, and save the file.
4. Create a CSV file from the downloaded template.

#### **CSV Format**

- Do not change the heading (first) row text.
  - Role Name is the only required field.
  - For any fields not used: Preserve all headings on the first row, but leave cells below blank.
5. In the **Import/Export Roles** window, select **Choose File** to select the file, and select **Import Roles**.  
The content of the file is added to the existing Role database. The new content does not replace the current database.
  6. Navigate to **Users, Manage Roles**, and confirm that the import was successful by inspecting the Roles list.

### **Export Roles and Role Groups**

A CSV list of all custom Roles can be downloaded by selecting **Export Custom Roles**. This exported file can be used to make a revised version, and then imported back into Privileged Access Manager.

## **Identify User Roles and Privileges**

Privileged Access Manager provides a preconfigured set of user roles. You can also configure your own roles from a set of available user privileges.

### **Predefined Roles**

A predefined set of 21 roles is provided with the product. View these roles by selecting **Users, Manage Roles**. This set has the privileges that are required to perform various common activities.

Roles are assigned to Users and User Groups during their creation and editing. See [Provisioning Users](#) for more information.

#### **Administrative Auditor**

Allow user read only access to administrative pages (services, users, devices, policies).

**Privileges:** servicesRead, usersRead, userGroupRead, socketFilterAgentRead, devicesRead, deviceGroupRead, policyRead, socketFiltersRead, commandFiltersRead, rolesRead

#### **Auditor**

Allow users to view PAM logging, session recording, and reporting data. Auditors have read-only access to Global Settings to inspect settings that have impact on log data.

**Privileges:** overviewRead, loggingAll, sessionRecordingRead, globalSettingsRead

#### **Autodiscovery**

Allow users to use the autodiscovery feature to find network devices.

**Privileges:** autodiscovery

#### **AWS API Proxy User**

Allow the user to log in, select the access page, and remotely access the AWS API Proxy.

**Privileges:** accessAll, awsApiProxy, manageAll

#### **CA TAP API User**

All the privileges that are needed for CA Threat Analytics to use the external API.

**Privileges:** accessAll, BAPApiManage, devicesRead, usersRead, sessionManage

#### **Configuration Manager**

Allow users to set "Global Settings" and access all "Configuration" tabs.

**Privileges:** globalSettingsRead, globalSettingsManage, configurationManage

**Delegated Administrator**

A combined user role that grants to users the ability to perform all User, Device, and Policy Manager tasks.

**Privileges:** usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, cacUserApproval, socketFilterAgentRead, socketFilterAgentDelete, devicesRead, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate, policyRead, policyManage, socketFiltersRead, socketFiltersManage, commandFiltersRead, commandFiltersManage

**Device and Device Group Manager**

Allow users to read, create, update, and delete all types of devices.

**Privileges:** socketFilterAgentRead, socketFilterAgentDelete, devicesRead, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate

**Global Administrator**

Allow access to all and configuration of all Privileged Access Manager functionality.

**Privileges:** accessAll, manageAll, monitorAll, sessionRead, sessionManage, overviewRead, toolsAll, loggingAll, sessionRecordingRead, globalSettingsRead, globalSettingsManage, servicesRead, servicesManage, servicesDelete, usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, cacUserApproval, socketFilterAgentRead, socketFilterAgentDelete, devicesRead, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate, policyRead, policyManage, socketFiltersRead, socketFiltersManage, commandFiltersRead, commandFiltersManage, policyImport, policyExport, configurationManage, rolesRead, autodiscovery, credentialsManage

**Global Setter**

Allow users to set "Global Settings".

**Privileges:** globalSettingsRead, globalSettingsManage

**Management Console API User**

Allow user access to CA Management Console API (Internal use only).

**Privileges:** managementConsole

**Monitor**

Allow users to monitor devices.

**Privileges:** monitorAll

**Operational Administrator**

Allow access to all PAM administrative functionality, without configuration management.

**Privileges:** accessAll, manageAll, monitorAll, sessionRead, sessionManage, overviewRead, toolsAll, loggingAll, sessionRecordingRead, globalSettingsRead, globalSettingsManage, servicesRead, servicesManage, servicesDelete, usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, cacUserApproval, socketFilterAgentRead, socketFilterAgentDelete, devicesRead, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate, policyRead, policyManage, socketFiltersRead, socketFiltersManage, commandFiltersRead, commandFiltersManage, policyImport, policyExport, rolesRead, autodiscovery, credentialsManage

**Password Manager**

Allow users to configure Password Management.

**Privileges:** credentialsManage

### ***Policy Manager***

Allow users to read, create, update, and delete all policies, socket and command filters, and agents.

**Privileges:** socketFilterAgentRead, socketFilterAgentDelete, policyRead, policyManage, socketFiltersRead, socketFiltersManage, commandFiltersRead, commandFiltersManage

### ***Secrets Management***

Allow users and user groups to access the Secrets Management functionality. Users with this role are still unable to see or manage any vaults or secrets until they are assigned a Vault Owner, Secrets Owner, or a Secret Viewer role for a vault.

See [About Secrets Management and Roles](#) for procedures on assigning these more granular roles.

**Privileges:** enableSecretsManagement

### ***Server Control Administrator***

Allow users to access the Server Control and UNAB policy management functionality.

**Privileges:** devicesRead, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate, deviceGroupDelete, deviceGroupAdd, loggingAll, usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, userGroupDelete, userGroupAdd, devicesRead, deviceGroupRead, servercontrolPolicyManage, servercontrolPolicyRead, servercontrolPolicyDeploy, servercontrolPolicyDeployRead, UNABManage, servercontrolPolicyAuditRead

### ***Server Control Deploy Manager***

Allows full access to policy deployment features, including assign, unassign, upgrade and downgrade; Read only access to server control policies and devices/device groups.

**Privileges:** devicesRead, deviceGroupRead, servercontrolPolicyDeploy, servercontrolPolicyRead, servercontrolPolicyDeployRead, servercontrolPolicyAuditRead

### ***Server Control Policy Editor***

Allows user full access to server control policy create, updates, version, and finalization operations; Read only access to policy deployment and deployment audit features, and read only access to device/device groups. **NOTE:** This role is restricted from performing SC policy manage operations including Assign/Unassign, Upgrade and Downgrade. This role is also restricted from performing any UNAB operations.

**Privileges:** servercontrolPolicyManage

### ***Service Manager***

Allow users to read, create, update, and delete service.

**Privileges:** servicesRead, servicesManage, servicesDelete

### ***Session Manager***

Allow users to view and terminate PAM login and remote access.

**Privileges:** sessionRead, sessionManage

### ***Standard User***

Allow users to access and manage remote devices.

**Privileges:** accessAll, manageAll

### ***Target Connector Validator***

Enables users to view and use the Target Connector Framework validator. The validator examines UI definitions from a JSON file, which renders pages for custom target connectors.

Privilege: `validateTargetConnectorUI`

### **Troubleshooter**

Allow users to access the "Configuration, Tools" page.

**Privileges:** `toolsAll`

### **UNAB Manager**

Allows full access to UNAB Host Login Policy management and UNAB Configuration Token management on devices and device groups.

**Privileges:** `devicesRead, UNABManage, devicesManage, devicesDelete, devicesAssign, deviceGroupRead, deviceGroupUpdate, deviceGroupDelete, deviceGroupAdd, usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, userGroupDelete, userGroupAdd, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, userGroupDelete, userGroupAdd`

### **User and User Group Manager**

Allow users to read, create, update, and delete all types of users.

**Privileges:** `usersRead, usersManage, usersDelete, usersAssign, userGroupRead, userGroupUpdate, cacUserApproval`

### **VMware NSX API Proxy User**

Allow the user to log in, select the access page, and remotely access the VMware NSX API Proxy.

**Privileges:** `accessAll, manageAll, nsxApiProxy`

### **Privilege Definitions**

In addition to the set of predefined roles, administrators can also create custom roles. A role is constructed by selecting from a list of Privileges, described in the following table.

Role Privilege	Actions Allowed
<b>Standard User</b>	
<code>accessAll</code>	Use the access page to connect to remote machines.
<code>manageAll</code>	Use the manage devices page to perform actions like power cycling remote machines.
<b>Monitoring</b>	
<code>monitorAll</code>	Use the monitor page to view the status of remote devices.
<b>Sessions</b>	
<code>sessionRead</code>	Look at the manage sessions/logins page.
<code>sessionManage</code>	Use the manage sessions/logins page to kill sessions and logins.
<code>overviewRead</code>	Examine devices, out of band devices, and connections.
<b>Tools</b>	
<code>toolsAll</code>	Use configuration tools such as ping and traceroute.
<code>validateTargetConnectorUI</code>	Use the Target Connector Validator for TCF custom connectors.

<b>Logging / Recordings</b>	
loggingAll	Look at the log page and execute reports.
sessionRecordingRead	Replay session recordings.
<b>Global Settings</b>	
globalSettingsRead	See global settings.
globalSettingsManage	Alter global settings.
<b>Services</b>	
servicesRead	See details of all services, of any type (TCP, RDP Application).
servicesManage	Add or change any existing services of any type (TCP, RDP Application).
servicesDelete	Delete any existing services of any type.
<b>Users</b>	
usersRead	See details of all users. Allows export of users.
usersManage	Create or change users including export. Allows import of users.
usersDelete	Delete any non-LDAP users.
usersAssign	Assign a user to a user group or a user group to a user.
userGroupRead	See details of user groups.
userGroupUpdate	Change existing user groups, but not their memberships.
cacUserApproval	Approve candidate CAC users.
rolesRead	Read roles and privilege definitions.
<b>Socket Filters</b>	
socketFilterAgentRead	View socket filter agents.
socketFilterAgentDelete	Delete socket filter agents.
socketFiltersRead	See socket filter lists and configuration.
socketFiltersManage	Change or remove socket filter lists and configurations.
<b>Devices</b>	
devicesRead	See details of all devices, including power hosts and consoles. Allows export.
devicesManage	Create and change devices and their memberships. Allows import.
devicesDelete	Delete any devices.
devicesAssign	Assign a device to a device group or assign a device group to a device.
deviceGroupRead	See details of device groups.
deviceGroupUpdate	Change existing device groups, but not their memberships.
autodiscovery	Find devices on the network.
<b>Policy</b>	
policyRead	See policies. Do not allow export.
policyManage	Change or remove policies. Do not allow import.
policyImport	Import all kinds of associations.

policyExport	Export all kinds of associations.
<b>Command Filters</b>	
commandFiltersRead	See command recording lists and configuration.
commandFiltersManage	Change or remove command filter lists and configurations.
<b>Configuration</b>	
configurationManage	Use the Access configuration tab.
<b>Passwords</b>	
credentialsManage	Create and update credential definitions for password chaining.
<b>APIs</b>	
awsApiProxy	Allow access to the AWS (Amazon Web Services) API Proxy.
BAPApiManage	Manage the CA Threat Analytics API.
managementConsole	Manage the Management Console API.
nsxApiProxy	Allow access to the VMware NSX API Proxy.
<b>Server Control and UNAB Policies</b>	
servercontrolPolicyManage	Read, create, update, copy, finalize, and delete Server Control policies and their versions
servercontrolPolicyRead	Provides read-only access to Server Control policies and their versions
servercontrolPolicyDeploy	Provides access to deployment operations for Server Control Policies, including Assign, Unassign, Upgrade, and Downgrade
servercontrolPolicyDeployRead	Provides access to view the policy device and device group assignments, including Server Control Policies, devices, and device group assignments
UNABManage	Provides access to UNAB operations, including read, create, update, copy, and delete UNAB Host Login Policies, and UNAB Configuration Token management, including read, created, update and delete of UNAB configuration tokens on devices a device groups
servercontrolPolicyAuditRead	Provides read access to the Server Control Deployment Audit Log entries

**NOTE**

- [User Roles](#)

## Create and Manage Users

As an Administrator, follow these procedures to create or edit Users. Create and modify user records using a template or a CSV file. For LDAP or RADIUS groups, you can only modify existing user records.

Review the following ways to managing users:

### Add a User Account Using the Template

Create a user account using a template in the UI. The configurable characteristics for each user include:



- Basic profile information
- User authentication methods and the status of the user account
- Roles that define user privileges
- Time restrictions for user login
- User group membership
- API Keys

If you are updating an existing user account, a **Manage Policy** button is available. Select this button to navigate to the Policy page, but changes already made to the user record are lost. Populate the User(Group) field there with the current user name.

### ***Specify Basic Information***

Provide user name and contact information in the **Basic Info** section.

#### **Follow these steps:**

1. Log in to the UI.
2. Select **Users, Manage Users**.
3. Select **ADD** to create a user.  
A user account template appears in the list window.
4. Complete the fields on the **Basic Info** tab. Required settings are indicated by a red asterisk. Note the following information about some of the fields:
  - **User Name:** Accepts alphanumeric characters, dashes (-), underscores (\_), and spaces. For AWS users, a user name can be from 2 through 32 characters long because of restrictions on federated users within AWS.
  - **Password:** The user password

### ***Configure Administration Settings for the User Record***

The Administration tab contains information indicating how a user authenticates and the status of that user account.

#### **Follow these steps:**

1. Select the **Administration tab**.
2. Select an authentication method for the user from the menu in the Authentication field:
  - **Local:** Local user accounts are hosted in the PAM database.
  - **RADIUS:** User authenticates to a RADIUS server. The user enters credentials that are provisioned by the RADIUS server. This option is available only if a RADIUS server is configured (see **Configuration, 3rd party**). If a RADIUS User is provisioned through LDAP, that user authenticates against a RADIUS server.
  - **RSA:** Authentication with an RSA SecurID. Users log in with a name and passcode. The passcode is a combination of the personal identification number and the current readout from the SecurID device. For example, if your PIN is 3425 and the current readout from your SecurID device is 866329, the passcode is: 3425866329
  - **Smartcard/PKI** - User authenticates with a Smartcard. PAM checks the user certificate against an OCSP server, or a Certificate Revocation List (CRL). The first time that a Smartcard user accesses the server, the Designated Name, and User account is registered. The User name appears in the **Approve CAC User** tab. This user must be approved before device access can be assigned.  
To use Smartcard authentication, set the Smartcard parameters in the **Security, Access, PKI Options**.
3. Configure the deactivation and termination settings for the user account.
4. If you select the **Terminate Session on Account Expiration** check box, a user login and all current sessions are terminated at the expiration date/time or the account violation limit is exceeded. If a user account is deactivated while that user is logged in, the session is terminated.
5. Specify email accounts to receive notices when the configured user logs in. The **Email on Login** field triggers an email to a specific administrator. The **Email Self on Login** field triggers an email to the address in the Basic Info section of the user record.

6. If the user is accessing Privileged Access Manager from the PAMClient, enter a range of IP addresses permitted to log in. Delimiters that are permitted include the space, comma, semicolon, newline. Both IPv4 and IPv6 address formats are supported and can be combined.

IP address formats permitted include:

- Single IP: 192.0.2.1 (IPv4), fd6d:8d64:af0c:1:0:242:22:233 (IPv6)
- CIDR: 192.0.2.0/28 (IPv4), fd6d:8d64:af0c:1:0:242:22:233/64 (IPv6)
- Range: 192.0.2.1-32 (IPv4), fd6d:8d64:af0c:1:0:242:22:1-ffff (IPv6)

If this field is empty, no IP address restrictions are applied. The user definition overrides the User Group definition. If no user policy is defined but that User is a member of multiple groups with different rules, the group permissions are additive (less restrictive).

#### NOTE

If your PAM server sits behind a networking device, such as a proxy, load balancer, or router, ensure that the device prevents against IP spoofing of the X-Forwarded-For HTTP header.

### ***Assign Access Roles to the User***

An access role is a collection of access-defined privileges. To perform access operations, each user must be assigned one or more roles.

Before you can assign roles to a user, the roles must be defined in the **Users, Manage Roles** list. To define roles, see [User Roles](#).

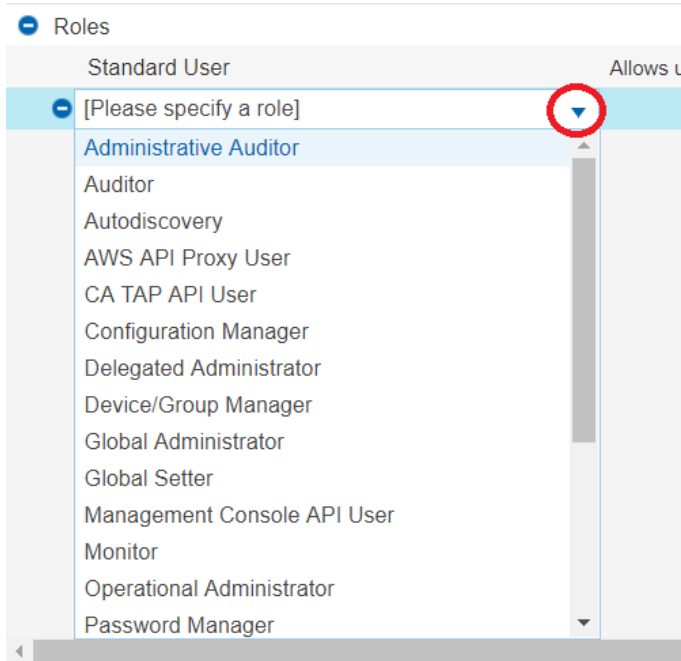
#### **Follow these steps:**

1. On the **Add** or **Update** user screen, select the **Roles** tab.
2. If necessary, expand the Roles list by selecting the plus sign to the left of the Roles table.  
"Standard User" is the default preassigned role. This role allows device access.

#### NOTE

The user can also inherit roles from Groups of which they are a member.

3. Do the following steps for each role that you want to assign:
  - a. Select the plus sign (+) to the right.
  - b. Select the **Please specify a role** field that appears, then select the caret symbol (highlighted in the following screenshot) to open a pull-down list of available roles.



- c. Select a role from the list to assign it.

If a role (for example Device/Group Manager or Policy Manager) requires you to specify the User Groups, Device Groups, or both, over which the role has control, corresponding entries appear below the role.

**To specify such groups, use one of the following options:**

- Select the plus (+) icon to the right of the entry to specify a required group.
- Select the **[Please specify a group]** entry that appears to open the **User Groups** or **Device Groups** selection dialog (as appropriate), as shown in the following screen capture:

## User Groups

☐ All Users

User Groups: \*



OK

Cancel

- Select **All Users** to include all user groups, start typing in the **User Groups** field, or select the magnifying glass icon to open a dialog with comprehensive search options.

### NOTE

You can only select one user or device group at a time. To specify additional groups, use the + option to the right of **User Groups** or **Device Groups** entry, as required.

After you have selected a group using any method, select **OK** to save it.

### NOTE

To provide a user with access to Credential Manager functions, add the **Password Manager** role.

Each user with Credential Manager access must also be assigned one or more predefined *Credential Manager groups* to determine the credential management functions they can access. For more information, see [Add Credential Manager Roles and Groups](#).

## Specify Login Time Periods

You can configure time-based access restrictions that determine when a user can log in to the server, select the **Access Times** option.

**Follow these steps:**

1. From the UI, select **Users, Manage Users**.
2. Add or modify an existing user entry.
3. Select the **Access Times** tab.
4. Select the plus sign then specify the days when to allow access.
5. In the **From** and **To** table columns, select the drop-down list to display a list of times. Access times are specified in UTC.
6. Select **OK** to save your entries.

**Add Users to Groups Including Credential Manager Groups**

Before a user can become a member of a user group, that group must be set up. Set up user groups by selecting **Manage Users, Manage User Groups**. After the group is configured, add users.

Follow these steps:

1. Open the User record.
2. Select one of the appropriate Group tabs:
  - **Groups**: Accessible by users with any roles unless they only have the Password Manager role, in which case the tab is grayed out.
  - **Credential Manager Groups**: Accessible by any user with the Password Manager role. Otherwise, the tab is grayed out.
3. To add the user to one or more groups, select the checkbox for each group.
4. Select the right arrow to move the groups to the Selected Groups list.
5. Select **Save**.

**NOTE**

User groups are not available for Active Directory or other directory users. Instead, users should be grouped in the directory and the attribute that is read by Privileged Access Manager. Setting policies for directory users is done at the group level.

**Grant Access to the External REST API**

The External REST API provides programmatic control over most PAM functions. The API uses HTTP basic authentication with API keys (secured using HTTPS) for user authentication. Authorization is provided by associating API keys with roles that determine privileges.

Assign API Keys and configure role assignments on the **API Keys** tab. For complete procedural information, see [Grant External REST API Access to Users](#).

**Configure Extended Identities**

Configure alternate accounts to access RDP applets, mainframe applets, Azure SQL Managed Instances and Azure AD instances on the **Extended Identities** tab.

**NOTE**

The Extended Identities are disabled during your initial login session or when logged in after being required to change your password.

To specify an alternate account, enter it in the corresponding **Value** field:

- **RPD User Name:** Enter the an account name for use by the RDP Applet or the MSSQL JIT target connector.
- **Mainframe Display Name:** Specify an account name to use to access the AS/400 applets (TN5250 and TN5250SSL).
- **User Principal Name:** (Imported LDAP users only) Provides an account name that can be used to access an Azure SQL Managed Instance.

**NOTE**

**User Principal Name** is read-only, populated with the value of the `User Principal Name` attribute (if present) from the LDAP record of the imported user.

- **Azure Username:** Specify a valid Azure AD account name (an email address) to use to access an Azure SQL Managed Instance. The specified value must be an account that already exists in Azure AD.

### **Edit User Records in LDAP or RADIUS Groups**

These user records are created through features in the **Users, Manage Groups** page. However, portions of their records can be edited on the **Manage Users** page. Note these characteristics:

- The user is already assigned (the copy of) the LDAP group it was imported from (see **Groups** panel).
- No fields that are imported from LDAP or RADIUS can be edited.
- You can edit certain assigned fields, including:
  - Keyboard Layout
  - RDP Username
  - Mainframe Display Name
  - Account Status
  - Terminate Session Upon Deactivation
  - Email on Login
  - Email Self on Login
  - Available Roles
  - The Access Time fields
  - Available Groups (the associated LDAP group cannot be removed).

### **Edit User Records from a Policy**

An administrator can edit a user record directly from the Manage Policies page.

1. Open the **Policies, Manage Policies** page.
2. Select **ADD** or **UPDATE**.
3. Populate the User (or Group) field with a record name.
4. Select **Manage User** to open the User record.
5. Open the User record.
6. When finished, select **Manage Policy** to return to the Manage Policies page.

## **Configure User Groups**

To combine users with similar attributes, define a user group. User groups allow for more manageable changes. Each user can be a member of one or more user groups. User group settings override the same individual user setting.

The following sections describe user group types and how to configure groups:

### **User Group Types**

- **Access User Groups**

Access User Groups are static collections of Users. Some User attributes, such as (Access) Roles and Access Time, can be assigned at the group level.

- **Credential Manager User Groups**

Credential Manager user groups are dynamically determined. User groups are based on a Credential Manager role and a Target or Request Group of the current set of users. Create these User Groups by navigating to **Policy, Manage Passwords, Users, User Groups**.

- **Local Groups**

Local groups are a collection of local users.

#### NOTE

Do not confuse Access user groups with Credential Manager user groups. User groups and roles are specified in two distinct locations, one for general use and one specifically for Credential Managers

### Use the UI Template to Create a Group

To create a user group consisting of local users, use the UI template. The instructions for each part of the template are explained.

#### **Basic Info Configuration**

##### **Follow these steps:**

1. Log in as an appropriate administrator.
2. Select **Users, Manage User Groups**.  
A User Group is necessarily restricted to a single Authentication scheme.
3. Select **Add** to create a local or SAML group.  
For RADIUS, TACACS+, and LDAP groups, see the relevant instructions.
4. Complete the fields in the **Basic Info** tab. Note the following information:
  - **Group Name:** Double-byte characters are allowed.
  - **Applet Recording Warning:** Set this option to **Yes** to display a notification that an applet (such as SSH or RDP) session is being recorded. (This option is ignored for TCP/UDP and RDP service sessions.) For example, when a user who is a member of the group opens an SSH applet console, the following warning appears in the title bar of the window and in the first line of console: **"Warning you are being monitored."**

#### NOTE

The related **Show Recording Warning** setting on the **Settings, Global Settings** page **Warnings** tab is ignored for applet sessions that are made by users who are a member of any group for which **Applet Recording Warning** is enabled. The global **Show Recording Warning** setting applies for all applet sessions that are made by users who are not members of any group and for *all* TCP/UDP and RDP service sessions.

If a user group is imported from an LDAP directory, the Group Name has the following format:

- From Active Directory: LDAPsourceGroupName + "@" + *LDAP\_domain*. The *LDAP\_Domain* is the base DN in the **Bind Credentials** field of the LDAP Domain configuration (**Configuration, 3rd Party, LDAP**).
- From other LDAP directory servers, such as OpenLDAP: LDAPsourceGroupName

Also, the **Description** field has the format: "LDAP Group" + LDAPsourceGroupName + "from" + LDAPsourceDistInUlshedName

#### **Administration Configuration**

The Administration section is where you specify the user authentication method

##### **Follow these steps:**

1. Select the **Administration** tab.

2. In the **Authentication** field, select an option from the drop-down list. The available options depend on which type of group is being created (Local, RADIUS, or imported LDAP).

If you select SAML as an authentication method, the user authenticates by a SAML assertion. The SAML attribute depends on the user provisioning source:

**For Active Directory:**

- Distinguished Name
- User Principal Name
- SAM Account Name

**LDAP directory like OpenLDAP or other:**

- Distinguished Name
- Unique Attribute

**If Authentication method is Local, RADIUS, or PKI:**

- User Name

3. If the user is accessing the server from the PAM Client, enter a range of IP addresses that are permitted to log in. Delimit each address with either a space, comma, semicolon, or newline. Both IPv4 and IPv6 address formats are supported and can be combined.

IP address formats permitted include:

- Single IP: 192.0.2.1 (IPv4), fd6d:8d64:af0c:1:0:242:22:233 (IPv6)
- CIDR: 192.0.2.0/28 (IPv4), fd6d:8d64:af0c:1:0:242:22:233/64 (IPv6)
- Range: 192.0.2.1-32 (IPv4), fd6d:8d64:af0c:1:0:242:22:1-ffff (IPv6)

If this field is empty, no IP address restrictions are applied. The user definition overrides the User Group definition. If no user policy is defined but that User is a member of multiple groups with different rules, the group permissions are additive (less restrictive).

**NOTE**

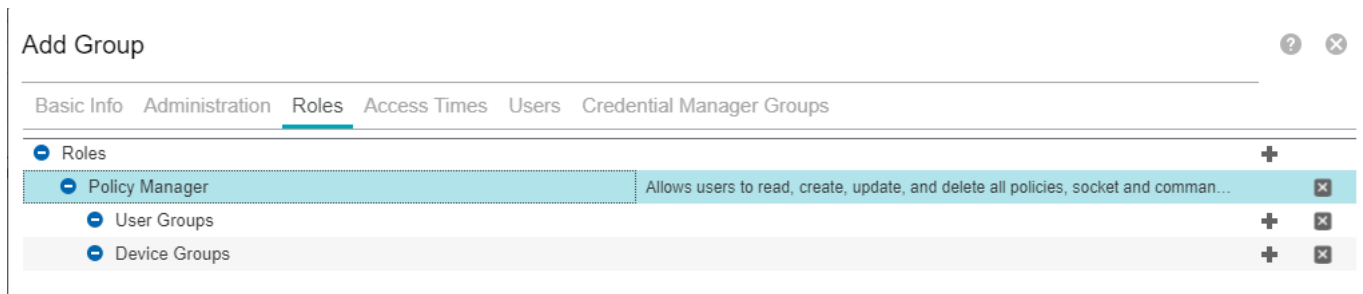
If your PAM server sits behind a networking device, such as a proxy, load balancer, or router, ensure that the device prevents against IP spoofing of the X-Forwarded-For HTTP header.

**Define Roles for a User Group**

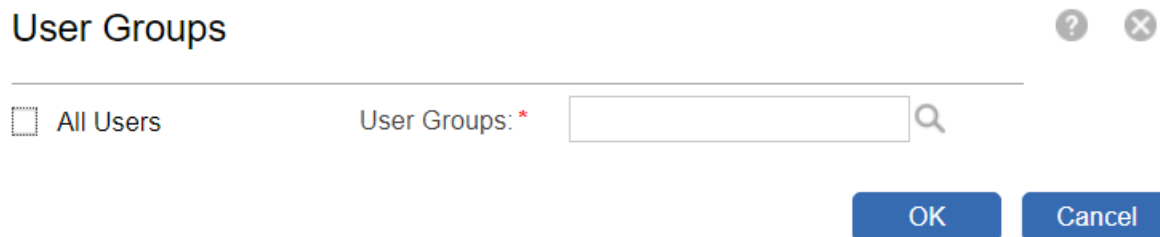
Multiple roles can be assigned per group. The standard user is the default role.

**Follow these steps:**

1. From the **Add Group** screen, select **Roles**.
2. Expand the **Roles** list using the plus sign.  
The Standard User is the default preassigned role. This role allows device access.
3. Select the plus sign to the right and a new line displays prompting you to specify a role.
4. Select the **Please specify a role** field. Select the arrow for a pull-down list that becomes available.  
The list shows all currently defined roles and a set of predefined roles.
  - Specify a role using the **Available Roles** drop-down list.
  - If an access role has the Credential Manager permission, this role can provide access to the Credential Manager menu from the Policy, Manage Passwords selection. You must specify a Credential Manager user group to determine the scope of menu access. Use the expansion pane Credential Manager Groups.
  - If a role (for example Device/Group Manager or Policy Manager) requires you to specify the User Groups, Device Groups, or both, over which the role has control, corresponding entries appear below the role, as shown in the following screen capture:



Select the plus (+) icon to the right of the entry to specify a required group. Select the **[Please specify a group]** entry that appears to open the **User Groups** or **Device Groups** selection dialog (as appropriate), as shown in the following screen capture:



Select **All Users** to include all user groups, start typing in the **User Groups** field, or select the magnifying glass icon to open a dialog with comprehensive search options.

#### NOTE

You can only select one user or device group at a time. To specify additional groups, use the + option to the right of **User Groups** or **Device Groups** entry, as required.

After you have selected a group using any method, select **OK** to save it.

### Credential Manager Role Inheritance

The ability to map Credential Manager User Groups to Access Manager User groups enables role inheritance rather than assigning a Credential Manager Role for each user.

#### Follow these steps:

1. Go to **Users, Manage User Groups**.
2. Select **Update User Groups**.
3. Select the **Credential Manager Groups** tab.

Assign a Credential Manager group to an Access Manager group that has a role with the **Manage Credentials** privilege. You are not limited to the set of preconfigured roles in PAM for either Credential Manager or Device Manager. You can customize the permissions for a role to ensure the lease privilege is maintained (a user can view credentials but not make changes to the account in firecall users) Three roles included with PAM that contain the Manage Password Privilege are Global Administrator, Operational Administrator, and Password Manager.

If you attempt to do a Save and select OK without adding a Credential Manager group, an error occurs with the following message:

"Roles with the Manage Credential privilege must have at least one Password Authority group to manage."

When upgrading to PAM 3.4 from an earlier version, no changes are made to Access Manager users, usergroups, role, or Credential Manager groups or roles.

#### NOTE

PAM users not explicitly assigned to any **Credential Manager Group** always become default members of the **Credential Manager Group** (CMGroup) named **Standard Users**. The **Standard Users CMGroup** has the



**FirecallUser** role with the **View Account Password** privilege. So, any member of **Standard Users** can view all target account passwords. This remains true even when the user might have inherited a CMGroup other than **Standard Users**, such as by means of a **Session Manager User Group (SMGroup)**.

The only way to prevent the user from viewing the target account password in this case is to explicitly assign the user the **Session Manager Role** with the **Manage Passwords** privilege; for example, assign the **Password Manager** role, and then add the user to a CMGroup (such as **Base Users**) that does not have **View Account Password** privilege. This removes the user from the **Standard Users** CM group. The user, therefore, no longer has the **View Account Password** privilege.

### ***Specify Time Periods for Group Login***

To configure time-based access restrictions when users in a group can log in to the server, select the **Access Times** option.

#### **Follow these steps:**

1. Add an entry to the **access times table**.
2. Specify the days and times for the access entry. the **From** and **To** table cells to display a drop-down list of times.
3. Select **OK** to save your entries.

### ***Add Users to Groups***

After the group is configured, add users.

#### **Follow these steps:**

1. Select the check box next to any user you want to add to the group.
2. Select the right arrow to move the groups to the Selected Users list.  
For Imported LDAP groups, users cannot be added or removed. Modify user records in the source LDAP directory.
3. Select **OK**.

#### **NOTE**

User groups are not available for Active Directory or other directory users. Instead, users should be grouped in the directory and the attribute that is read by Privileged Access Manager. Setting policies for directory users is done at the group level.

### **Elevate User Privileges Temporarily**

To elevate the privileges of a user temporarily, add them to a user group that has the additional privileges for as long as necessary. When the user no longer needs the elevated, simply remove them from that user group.

### **Create a RADIUS or TACACS+ Group**

You can create a user group that is imported from a RADIUS or TACACS+ server. For the RADIUS or TACACS+ buttons to become active, first configure the RADIUS or TACACS+ server for access to Privileged Access Manager. See [RADIUS or TACACS+](#) for instructions on configuring RADIUS connectivity.

#### **Follow these steps:**

1. Open a template by clicking the relevant button:
  - **Create RADIUS Group**
  - **Create TACACS+ Group**
2. Complete each section of the template. The instructions are similar to creating a local user group.  
To locate users in a RADIUS or TACACS+ group, each group name you specify must match a corresponding group name or ID on the RADIUS or TACACS+ server. Privileged Access Manager uses the configured grouping to manage users.

The GroupID must match a corresponding group on the RADIUS or TACACS+ server. All the privileges that users maintain are derived from their group. Only users with a local account or whose group matches the group name in the UI is granted access. Contact the RADIUS or TACACS+ server administrator for the group name.

If a RADIUS group is provisioned but the user does not exist, a shadow RADIUS user is created. The shadow user is not visible in the user management screen or the user list.

### **Import an LDAP Group**

For information about importing an LDAP Group, see [Import LDAP User Groups](#).

### **Edit from the Manage Policies Page**

An administrator can edit a user group record by invoking it directly from the Manage Policies page.

1. Open the Policy, **Manage Policies** page.
2. Populate the **User (Group)** field with a record name.
3. Double-click the name to display its editing template in a shadow box window.
4. When finished, select **Save** (or Cancel) to return to the **Manage Policies** page.

### **SAML SSO with Juniper SA Using RADIUS Authentication**

See Network Configuration, SSO, Juniper Networks, Configure Privileged Access Manager for SAML SSO with Juniper SA using RADIUS Authentication.

For information about importing an LDAP Group, see [Import LDAP User Groups](#).

## **Import LDAP User Groups**

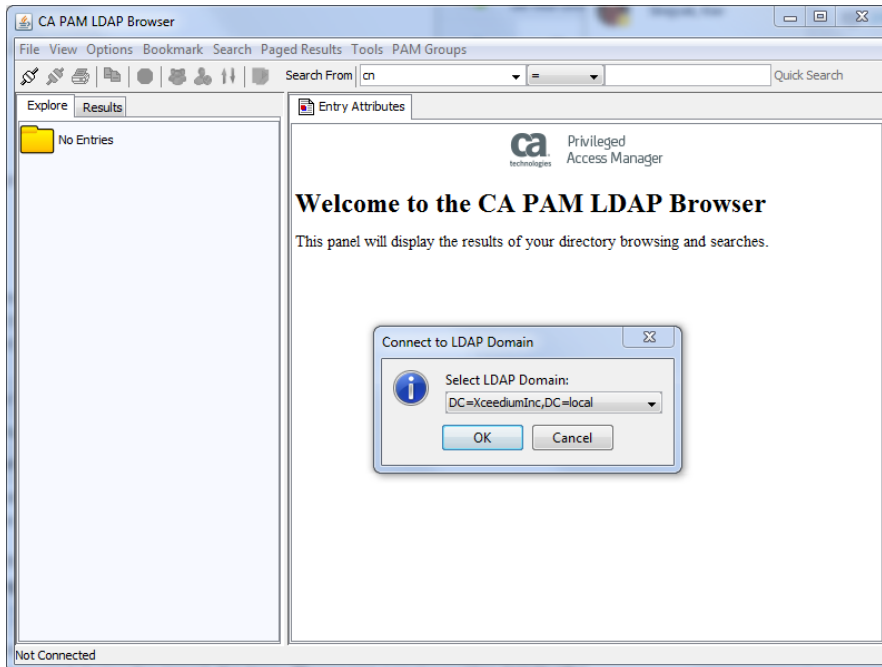
As an Administrator, an efficient method of creating an LDAP user group is to import an LDAP user group from a remote LDAP server. To import a user group, you must use the built-in *LDAP Browser*, which gets launched during the import procedure.

This topic explains the following tasks:

### **Launch the LDAP Browser**

To import LDAP Groups into Privileged Access Manager, follow these steps:

1. Verify that your appliance is licensed on the **Configuration, Licensing** page. A license is required to launch the LDAP Browser.
2. Navigate to **Configuration, 3rd Party, LDAP**, and configure access to an LDAP server. Provisioning the LDAP server is necessary to make LDAP groups available for import.
3. Select **Users, Manage User Groups**.
4. Select **Import LDAP Groups**.  
The LDAP Browser launches. You are prompted to select an LDAP domain.



## NOTE

Privileged Access Manager does not support SSH and LDAP connections from a native browser due to strong cryptography support. Update your local JCE with unlimited strength policy jars that are based on your JRE version.

5. Go to the next procedure to import the LDAP group.

If the LDAP server does not support the cipher suite that is used by the Privileged Access Manager LDAP browser, a connection failure occurs. The following error message appears: "Possible cipher mismatch with LDAP server." During provisioning, ensure that the ciphers that are supported on the target LDAP server include those ciphers that are supported by the LDAP browser.

## Import LDAP Groups

In the LDAP Browser, the **Explore** tab in the left pane shows a graphical representation of an LDAP tree. Select any object to see the object attributes.

### Follow these steps:

1. Select the LDAP domain and select OK to connect to it. The browser connects and displays all records below that domain.
2. Navigate the LDAP tree in the left pane and locate the user group that you want to import. Traverse the tree in any order or direction.
3. Select the user group to import.
4. Repeat these steps for each group you want to import.
5. (Optional) Review the user groups that are selected for import:
  - a. Select **PAM Groups, Manage selected groups to register with the PAM appliance**. The list of the Distinguished Names for all selected groups displays.
  - b. Select and edit any group DN, or remove it from the staging list.
6. Select **PAM Groups, Register selected groups with the PAM appliance**. A window opens displaying a list of the staged groups. You can watch the progress, and can display any messages that are associated with the actions.
7. When ready to import the groups, select **Register Groups** in the lower-left corner.

Privileged Access Manager imports the groups in the order that they are listed. The browser provides feedback and cancellation options throughout the process.

#### TIP

You can cancel registration of a group, or you can cancel the registration of all groups, even after they have started.

When the imports are finished, each line item in the registration window shows a green checkmark for success or a red **X** for import failure/cancellation.

8. (Optional) Review the status of the full list and each individual group by selecting its line item. If you made changes to an individual group or any errors occurred, the lower **Messages** panel provides details.
9. Go to **Users, Manage User Groups**, and confirm that the imported user groups appear on the page. Roles are inherited from the LDAP group. The default role is Standard User. Ignore the **Roles** panel, which indicates **"No roles selected."**

#### NOTE

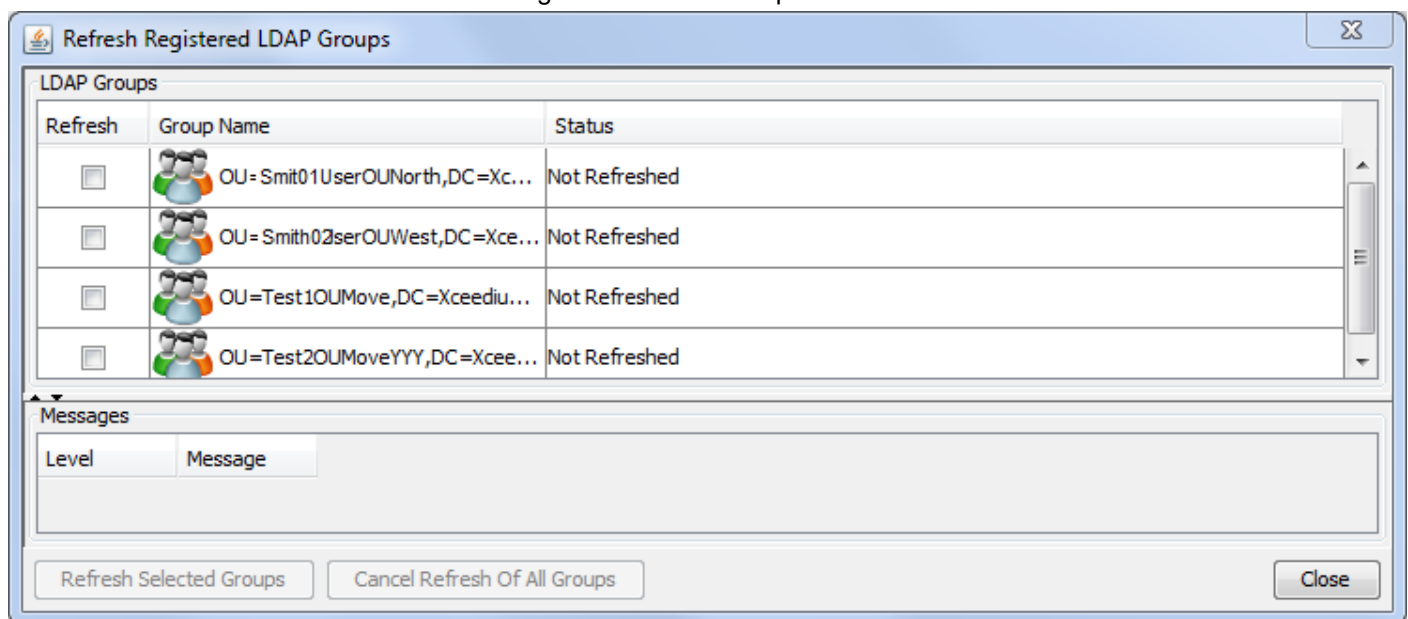
You cannot delete a record from an imported user group. Also, you cannot edit an LDAP-imported field.

### Refresh LDAP Groups

You can refresh an LDAP Group to update the records in the group.

#### Follow these steps:

1. In the UI, select **Users, Manage User Groups**.
2. Toward the right side of the page, select **Refresh LDAP Groups**.  
The LDAP Browser launches the Refresh Registered LDAP Groups window.



3. Select one or more groups you want to refresh and select Refresh Selected Groups.

### Refresh Active Directory User Groups After an OU Change

A change to organization unit (OU) of a user results in a change to the user DN. The modified DN can impact an access policy. PAM handles an OU change when the Active Directory group is refreshed automatically. During a refresh, the appliance searches the remote Active Directory Server and updates its user record. Despite the OU change, the policy for that user is preserved.

**WARNING**

To reflect an OU change immediately, you can manually refresh an Active Directory group in PAM. To keep the data in sync with Active Directory, refresh all the groups that now contain the user and all the groups from where the user moved.

**Nested Groups**

If an LDAP group is in a parent group **member** attribute, then users in the parent and child groups are imported with the parent. For example, consider groups CommunityA and CommunityB, and Person1. CommunityB is a member of CommunityA and it is nested in CommunityA. Person1 is the sole member of the group CommunityB. If you import the CommunityA group, you see every member of CommunityA and member Person 1 from CommunityB.

**LDAP Browser Menus and Controls**

The following table explains the LDAP Browser menus and controls options:

Text Menu	Function
Copy icon	Copy the Distinguished Name of selected entry to the Clipboard.
Group icon	Display all the groups in this container. After first selecting an object in the tree under the Explore tab, clicking this button will then switch you to the Results tab. Once there, you see a (fully expanded) tree of all groups (objectClass: group) contained within the selected object.
<b>File</b>	
Connect	Log in to an LDAP database. Invokes a pop-up window from which you can select from currently accessible domains.
Disconnect	Log out from the current LDAP domain.
Print	Print currently selected node.
Exit	Close browser window. The browser continues running while the connection is active. During that time, you can invoke the LDAP Browser by selecting Users, Manage Groups, Import LDAP Group.
<b>View</b>	
Show Button Bar	Icon-based menu Default: On
Show Search Bar	Icon-based menu Default: On
<b>Options</b>	
Set LDAP Connection Timeout	Maximum time (seconds) before a connection attempt is canceled. This timeout is useful when multiple servers are specified for a particular LDAP domain in <b>Configuration, 3rd Party</b> . Default: 60 seconds
Set Result Set Page Size	Maximum number of records in an LDAP directory before pagination is triggered for representation in the browser tree. Number of records in each page of a paginated subtree. Default: 1000
Enable/Disable Group Member SID Resolution	If enabled, resolve all members of security groups (including members of nested security groups) across domains.

<b>Bookmark</b>	A bookmark can be made on any leaf in a tree. You can select the bookmark later directly from the menu. Bookmarks are saved for each domain, and appear only when the browser is connected to that domain.
Add Bookmark	Opens an editing window for bookmarking currently selected leaf: <ul style="list-style-type: none"> <li>• DN – pre-populated with the current Distinguished Name (DN)</li> <li>• Bookmark Name – pre-populated with the current Common Name (CN)</li> </ul>
Edit Bookmark	Opens a bookmark selection window. Selection in turn opens a bookmark editing window (see Add Bookmark).
Delete Bookmark	Opens a bookmark selection window. Selection in turn deletes and confirms deletion of the bookmark.
<b>Search</b>	
Search Dialog	Opens a detailed search specification window. (Contrast to Quick Search.)
Delete Filter	Opens a window with a list of filters for selection and deletion.
Return Attribute Lists	
<b>Paged Results</b>	
Next Page of Results	Retrieve next page of results and display page wrapper (Page n Results) in the Explore tree (when green; otherwise, gray when inapplicable).
<b>Tools</b>	
Stop Action	Suspends current LDAP request. Stopping a request is useful when the page size is large and the browser is searching a large database.
Privileged Access Manager Groups	Privileged Access Manager-specific menu items
Manage selected groups to register with the appliance.	Lists all items that are currently selected (or staged) for importing to Privileged Access Manager.
Register selected groups with the appliance	Perform the input operation on the items that are selected, which are listed in Manage selected groups to register with the appliance.

## About Pagination

Pagination is available for Active Directory (AD) and OpenLDAP.

The LDAP Browser has a pagination feature to reduce overhead on LDAP access. The browser setting **Result Set Page Size** specifies the maximum number of members (directories, groups, or objects; or nodes) for any directory. (This value is initially set to a default of 1000.) If the overhead required to display all directory members is too heavy, the administrator can reduce this variable value.

For example, set this value to 5 to insert a pagination leaf for more than five members in any directory. The LDAP Browser inserts the initial pagination leaf is when that directory is opened, before displaying the actual directory contents.

## Search and Quick Search Options

If you know the name of the directory or object you are looking for, use one of two search options available in LDAP Browser. If the tree appears paginated in the browser, the search can still traverse the entire tree.

You can use the **Quick Search** button in the upper-right corner of the browser to locate the desired object.

**Follow these steps:**

1. In the **Explore** tab tree, select the node that you want to be at the top of the search.  
Your choice is reflected in the Quick Search label.
2. To the right of the Search From label, select an attribute from the drop-down list, and enter a search string in the text box.
3. Select **Quick Search**.  
A filtered tree appears in the **Results** tab.
4. Select an object in the tree to see **Entry Attributes** on the right.

**LDAP Browser Search Options**

To refine search results to a limited subset of objects or saved for future use, select menu item **Search, Search Dialog**.

The following table explains the search settings.

Field/Button	Definition
Filter Name	Assign a bookmark name for the filter: When you have filled in the remainder of this dialog, select Save in the lower right. The filter is then available from the Search menu.
Start Searching From	Identify the root node for your search.
<b>Alias Options</b>	
Resolve aliases while searching	When checked: LDAP Browser returns the real entry to which the alias points. When unchecked: LDAP Browser returns all alias entries as regular entries.
Resolve aliases when finding base object	
<b>Search Level</b>	
Select Search Level	Search Base Object Search Next Level Search Full Subtree
Information to retrieve	Allows you to select from a saved list in Return Attributes Lists.
<b>Filter Operators</b>	
Not	Negative of (entire) constructed entry
[Expression]	
[Attribute]	Menu of all LDAP attributes: accountExpires through x500uniqueIdentifier
[Operator]	Logic to apply to the attribute in this expression
[Character string]	Text being tested with this expression
More	Add another logic template to concatenate with other defined logic
Less	Remove most recently defined logic
Save	Save entire filled-in template to the label assigned in a filter name
Load	Load existing filter to this template for editing or copying.
View	Show the LDAP filter
<b>[Template Commands]</b>	
Search	Perform search as currently defined in this template.

Cancel	Close dialog without executing a search or saving it to a filter name
--------	---

### **Double-Byte Characters for User and User Group Names**

Privileged Access Manager provides double-byte character support. The appliance allows East Asian characters in data store and in the UI representation of user and user group names. LDAP user names are imported and displayed with the double-byte characters maintained.

User records with double-byte characters can be imported to LDAP groups but not to individual local user records.

## **Import and Export Groups**

### **NOTE**

You can create one CSV to import both Users and Groups rather than create one file for each page.

### **Add a Group from a CSV File**

#### ***Internet Explorer Requirements to Use a CSV File***

To use the Import/Export functions with Internet Explorer (IE), changes might need to be made to the security settings. To establish the necessary settings:

1. Open IE browser.
2. Select **Tools, Internet Options**.
3. In the Internet Options pop-up window, select the **Security** tab.
  - a. Select the slider zone.
  - b. Select **Custom level**. Scroll to **Downloads**. For **File download**, select the **Enable** option.
4. Select **OK** to save changes.

#### ***Import a CSV File***

To import the users, follow these steps:

1. Go to **Users, Manage User Groups**.
2. Select the **Import/Export** button.  
The Import/Export Users window appears .
3. Select Download Sample File, and save the file.
4. Create a CSV file from the downloaded template.

#### **CSV Format**

- Do not change the heading (first) row text.
  - New Group records:
    - For any fields not used: Preserve all headings on the first row, but leave the data cells blank.
  - Updates to existing Group records:
    - Each User Group is represented by a line record with Type="user group".
    - User Group records should be at the top of the file, ahead of all User records.
    - As it is for individual Users, an Authentication option can be applied to a User Group:
5. In the **Import/Export User Groups** window, select **Choose File** to select the file, and select **Import Users (User Groups)**.  
The content of the file is added to the existing User database. The new content does not replace the current database.
  6. Navigate to **Users, Manage User Groups**, and confirm that the import was successful by inspecting the User list.

### ***Export Users***



This button creates a CSV file of all Local, RADIUS, SecurID, and Smartcard/PKI users. For Local users, the **Password** field is masked.

#### NOTE

Whether you export a CSV from the Users or User Groups page, the same data is produced, including Users and User Groups.

## Manage User Accounts

Use the **Session Manager Users** panel, which lists all existing local, LDAP, RADIUS, and SecurID user accounts, to perform the following account management functions:

- [Add a User](#)
- [Edit a User](#)
- [Copy a User](#)
- [Disable a User](#)
- [Reactivate Accounts Disabled by Inactivity](#)
- [Delete a User](#)
- [Approve CAC Users](#)

#### NOTE

Imported LDAP values cannot be edited, but PAM-generated fields can. Smartcard/PKI user accounts can only be edited or deleted.

### Access the Session Manager Users Panel

To access the **Session Manager Users** panel, select **Users, Manage Users**.

#### Add a User

For information about adding users, see [Create and Manage Users](#).

#### Edit a User

Use this procedure to edit a user account.

#### To edit a user account, follow these steps:

1. On the **Session Manager Users** panel, select the line item record of the user account that you want to edit.
2. Select the **Update** button.
3. Edit the account details as required in the **Update User** dialog that opens.
4. Select the **OK** button to commit your changes.

#### Copy a User

Use this procedure to duplicate an existing user account to create a user account with the same access permissions and policies.

#### Follow these steps:

1. On the **Session Manager Users** panel, select the line item record of the existing user account that you want to duplicate.
2. Select the **Copy** button.  
A **Copy User** dialog that is populated with all the information of the original user account except for the username and password opens.

3. Do the following steps in the **Copy User** dialog:
  - a. Enter a username for the new account in the **User Name** field.
  - b. Enter an account password and confirm it in the **Password** and **Confirm Password** fields.
  - c. Optionally, change the other properties, as required.
  - d. Select the **OK** button.

The new user account is created and added to the list.

### **Disable a User**

Use this procedure to disable (preserve, but not allow activity by) a user account.

#### **Follow these steps:**

1. On the **Session Manager Users** panel, select the line item record of the user account that you want to disable.
2. Select the **Update** button.
3. On the **Update User** dialog that opens, select the **Administration** tab and deselect the **Account Enabled** option.
4. Select **OK**.

#### **To list disabled user accounts:**

Use the filters at the top left of the **Session Manager Users** panel:

1. Select **Account Enabled** from the **Column** drop-down list.
2. Select **False** from the **Value** drop-down list.
3. Select the **Filter** button to display only disabled user accounts.

#### **To reenable multiple user accounts:**

1. Use the filters at the top left of the **Session Manager Users** panel to display the disabled accounts:
  - a. Select **Account Enabled** from the **Column** drop-down list.
  - b. Select **False** from the **Value** drop-down list.
  - c. Select the **Filter** button to display only disabled user accounts.
2. Select individual users, or select them all by selecting the checkbox above the list to the left of the column headings.
3. When the list of choices is complete, select the **Enable** button.

### **Reactivate Accounts Disabled by Inactivity**

As an administrator, you can list user accounts disabled due to inactivity, and then reactivate some or all accounts. This bulk reactivation can help when multiple deactivated users request account reactivation.

#### **NOTE**

As an Administrator, you can also double-click individual users in the **Session Manager Users** page to display why the user is deactivated: Double-click a user to display the **Update User** window, and then find the reason in the **Administration** tab **Deactivation Reason** field.

The period after which users are disabled due to inactivity is specified in the Global Settings. For more information, see the [Accounts](#) section of the [Apply Global Settings](#) topic.

#### **Follow these steps:**

1. Use the filters at the top left of the **Session Manager Users** panel to display the deactivated accounts:
  - a. Select **Deactivation Reason** from the **Column** drop-down list.
  - b. Select **Inactivity** from the **Value** drop-down list.

#### **NOTE**

The **Other** value includes users who are actively disabled, or users disabled due to some sort of violation (for example: for violating command or socket filters).

- c. Select the **Filter** button. A list of user accounts disabled due to inactivity appears
2. Select the checkbox next to the **User Name** column heading to select all the users.
3. Select **Enable** to enable all selected users

#### NOTE

You can see the deactivation reason when you export users to a CSV file. The deactivation reason is also included in the response when adding or updating a user using the external REST api or the CLI. In all these cases, the deactivation reason is reported as an integer with the following values:

<u>Deactivation Reason</u>	<u>Numeric Value</u>
Other	0
Inactivity	1

#### Delete a User

To delete (completely remove) a user account, follow these steps:

1. On the **Session Manager Users** panel, select the line item record of the user account that you want to delete.
2. Select the **Delete** button.
3. Select **Yes** in the confirmation request. An acknowledgment is presented in a new dialog.
4. Close the acknowledgment box.

The user account is removed from the list.

#### Approve CAC Users

Smartcards, including Common Access Cards (CAC), use certificates to authenticate users. Privileged Access Manager validates the user certificate against a Certificate Revocation List. The smartcard parameters must be set in the **Global Configuration** under the **Security** tab.

The first time that a smartcard user accesses Privileged Access Manager their public key is registered and the user appears in the **Approve CAC User**. The user must be approved before device access can be assigned.

## User Viewing

#### Initial View

You log in to Privileged Access Manager initially as config, and then as super. When, as super, you switch over to the default Users menu, you see a list that is populated with the super account.

Later, you can view all and can edit any users here except for config. Config must be edited in the Toolbar: **Change Password** menu while logged in as config.

#### Filtering Populated User Views

After you have added users, they might not all be visible on the first Access page. If there is a large number, filter this set of users using the **Search** box to narrow the list to matches of the search string provided.

## Provision Access Policies

To enforce access rules for specific users and user groups. Policies for associating users and devices can be done at a granular level (device and port). Each user then has access only to devices and applications that they need to do their jobs.

A **policy** is a set of configuration values identifying permitted or required:

- **Access types** (access method applets, TCP/UDP, and application services)
- **Access restrictions** (command filters, socket filters)
- **Passwords** (which involve Devices and resident applications)
- **Recording** (graphical or command line)

A Policy specifies the interactivity between:

- one registered user or user group (including LDAP and RADIUS)

*and*

- one managed device or device Group

After a user logs in to a device using the policy assignments, the appliance can:

- Record user activity
- Perform command filtering
- Terminate user leapfrog attempts

### **Access Provisioning**

The access capabilities that you provide for a Device are available for specification in Policy. See [Set Up Access to a Target Device](#) for information about setting up access capabilities for Devices.

### **Access Restrictions**

Through a Policy, these restrictions to Device or Device Group access can be imposed on a particular User or User Group:

- Command Filtering
- Socket Filtering

### **Command Filtering**

You can use command filter lists to enforce policies in the command line applets TELNET, SSH, and serial consoles.

Both Command Filtering and Socket Filtering use whitelists and blacklists to set the appropriate policy.

- A command-filtering **blacklist** is a list of commands that a user *cannot* type. If the user attempts to type the command, the appliance can flag (log), alert, re-mediate, and stop the command from being processed. All other commands are allowed.
- A command filtering **whitelist** is a list of the commands that a user *can* type. All other commands are prohibited.

#### **NOTE**

Command filter whitelists cannot be configured for Mainframe TN3270 and TN5250 applets.

The Command Filter Configuration (CFC) sets the behavior of the blacklist and whitelist command filters.

### **Command Filter Alerts Example**

```
From: xsuitel@example.com
To: xs-admin1@example.com
Cc:
Subject: Alert Msg from xsuitel
```

```
-----
Date/Time: Fri, 1 Oct 2010 14:09:05
User ID: Traveler123
```

User Source IP: 168.0.2.123  
Violation on: LinuxBox12

Captured Keystrokes: rlogin

## **Socket Filtering**

Socket Filter Agents (SFAs) are Privileged Access Manager components that are used to restrict access either to server-based devices or from server-based devices. Socket filters provide a different kind of access control than devices with finite command sets, such as routers and switches, for which command filtering is applied.

Three components are required:

- Socket Filter Lists – to define either a socket blacklist (specifying where access is prohibited) or whitelist (specifying where access is allowed)
- Socket Filter Agents – to apply rules that are specified by Socket Filter Lists and used in Policies.
- Socket Filter Configuration – to apply agent behavior across all Privileged Access Manager-managed devices using socket filter agents.

### **Socket Filter Lists (SFLs)**

Socket Filter Lists define groups of servers or networks that can be applied to a policy for LeapFrog Prevention.

### **Socket Filter Agents (SFAs)**

Once a Socket Filter Agent is deployed and a user connects through Privileged Access Manager to the host Device, the SFA downloads the user policy. The SFA then enforces at the Device any blacklist or whitelist filters. A blacklist contains devices and ports that user is prevented from accessing. A whitelist identifies the only devices and ports that a user can connect to. The SFA does not inspect or disturb any other connections to that Device, such as production web traffic or Privileged Access Manager users who are not restricted.

SFAs can be installed on Windows and Linux devices. The Linux root account is exempt from SFA rules and restrictions. Windows administrator accounts are subject to SFA rules and restrictions.

### **Socket Filter Configuration (SFC)**

Global values that affect the behavior of the socket filter agents are found under Socket Filter Configuration, accessible through the Policies menu.

CA Technologies advises verifying your organization policies before setting up socket filtering. Network heartbeat checks might not be allowed.

## **Amazon Web Services (AWS)**

When connection is made to AWS after populating the Config, 3rd Party, AWS settings, the **Policy, Manage Policies, AWS Policies** link interface is established for specifying AWS IAM Policy.

### **Defining AWS Policies**

AWS policy is applied for AWS privileges when accessing the AWS management interface. Initially, the editing window **Manage AWS Policies** holds two default versions, but you can edit or create an IAM policy.

Although Privileged Access Manager is designed to pass an IAM Policy to AWS, AWS does not accept an **AWS Policy** that is "too lengthy." The length limit is not a predictable value, but can be evaluated by AWS before processing to avoid errors. Therefore, Privileged Access Manager sends all submitted policies to AWS for preprocessing. If the size limit is exceeded, an error message is relayed to the Privileged Access Manager user.

**Workaround:** Some guidance on permitted length is provided in this AWS Forum thread:

<https://forums.aws.amazon.com/thread.jspa?threadID=80882>

## Specifying AWS Policies

When a Service has been configured for access to the AWS management interface, the credential specification pop-up window in the Manage Policy interface also provides for the IAM policy specification through the **AWS Policy** field at the right-hand side of the pop-up window.

## Session Recording

In addition to the access controls that are applied in advance, session recording can be assigned to policy, providing a view of User actions after the fact. As recordings, they simulate the environment of the User to provide a view into what transpired during a connection session.

### NOTE

Privileged administrators also apply control during sessions with the ability to terminate a connection session or log a User off Privileged Access Manager, while Privileged Access Manager logging is another during, or post, session tracking resource.

In the command-line applets, TELNET, SSH, and Console user keystrokes can be recorded. Graphical session recording is available with the RDP and VNC applets.

Recordings are identified in the GUI as line items. They can be searched with variable text filtering. When a recording identifies a User violation, this fact is marked inside the recording as the User views it. The line item record is also highlighted in bold red.

The session recording logs are not stored on Privileged Access Manager. The session recording files can be stored on mount points or sent to a syslog consolidation server.

Use a directory mounted to a Windows or UNIX server for session recordings to be available through the administration interface. The session recordings can be viewed in **Sessions**, **Session Recordings**.

Session Recording policy is set for a user/user group – device / device group pair in **Policies**, **Manage Policies**.

In the **Recording** pane:

- Selecting **Command Line** records user entry, and if **Bidirectional** is selected, Privileged Access Manager records both the user and device responses.
- Selecting **Graphical** records the user GUI interaction with the Windows server as a movie that can be played, stopped at any point, and replayed from any point.

## Set Up a Policy

As an administrator, configure a policy to a user-device pair to define user access to the device.

Assign a policy using one of the following methods:

- [Policy template](#)
- [Imported CSV file](#)

A policy can also be applied based on inheritance from a parent group.

A user *effective policy* spans these categories, as the union of all policy assignments. It reflects the range of device and access options available to a user as represented on the **Access** page. As an administrator, you can view a user effective policy in **Users**, **Manage Users**, **Update**, **Manage Policy**.

### NOTE

PAM also dynamically adds devices and target accounts to the **Access** page of a user if those devices and target accounts are members of a Credential Manager target group that is referenced by a Credential Manager user group to which the user belongs. For more information, see [Dynamic Addition of Devices to the Access Page Based on Credential Manager Target Group Membership](#).

The configuration of a device provides a template for choosing which access methods are allowed for a particular user. The scope of this template has previously been defined by the attributes that are assigned in the device record.

A unique *policy* can exist between every match of each of the first (users and user groups) with each of the second (devices and device groups). For example, if there are three users and three devices, after matching each user with each device, there could be up to nine different policies. For information about overlapping policies, see [Overlapping Policies on Provision Access Policies](#).

#### NOTE

For information about Credential Manager password policies, see [Set Up Password Composition and View Policies](#).

### Prerequisites

- Session recording activation requires that storage be configured in advance on the **Configuration, Logs, Session Recording** page.
- The components of the policy are defined first so that they are available to include in a policy. Define users, devices, access types, services, and filters.

### Policy Template

Create an association with a user and device using the policy template. To import policies using a CSV file, see [Import or Export Policies](#).

These procedures begin from the Policy menu. However, for some user records, you can edit a policy template from the user record by selecting **Manage Policy**.

#### Follow these steps:

1. Select **Policies, Manage Policies**.
2. Complete *one* of the following actions:
  - Create a new policy by clicking **Add**.
  - Select an existing policy record and click **Update**. If the policy record is not listed, find it by selecting the User/User Group or Device/Device group search criteria at the top of the screen.
3. If you are adding a new policy, use the fields in the **Association** section to locate the user or device that you want to associate in a policy.
4. For the **User** or **User Group** field, use the search icon to display the list of choices, and select the matching full name from the drop-down list. Select **OK**.
5. For the **Device** or **Device Group** field, use the search icon to display the list of choices, and select the matching full name from the drop-down list. Select **OK**. If you select a device group, only those access methods that are specified for the group are displayed.
6. On the **Access** tab, select one or more entries from the list and move it to the Selected Access list.
7. On the **Services** tab, select one or more services available for a provisioned device.
8. On the **SAML** tab, set SAML options as appropriate. (SAML must already be configured for anything to show here.)
9. On the **Password** tab, select the passwords the user or user group can manage. Then, select from the available device or device group defined target applications. When you select a target application, you can also select one or more provisioned target accounts for that application that the user can manage. For AWS AMI instance on UNIX and Linux devices, only EC2 keys auto-populate as options.
10. If Socket Filter Agents are installed in the environment, select the available command and socket filters to assign to the black and white lists on the **Filters** tab. The filters that are listed are those that are configured in the **Filters** option of the UI. Select the **Restrict login if agent is not running** check box.

- If the product cannot detect a running SFA on the device and an SFA-monitored connection is attempted, the login is rejected. Unmonitored connection instances are never rejected by selecting this option.
  - SFAs monitor the following connections: Access Method GUI, CLI, and mainframe applets; and RDP, VNC, and ICA Services.
  - SFAs do not monitor: standard (customized) Services and Web Portal Services.
11. If [session recording capability is configured](#), specify the types of recording to make using the options on the **Recording** tab. Set one or more of the following available options (availability depends on the selected access methods on the **Access** tab):
- **Graphical** (available for RDP and VNC access methods): Record user activity graphically.
  - **Command Line** (available for TELNET, SSH, and Console access methods): Record user activity on the target device as plain text.
    - **Bidirectional** (applicable for command-line recordings only): Record command-line output from the operating system or application and input that the user types. Bidirectional recording is required for SSH Proxy applets. All mainframe-access applets apply bidirectional session recording when you enable recording.
  - **Web Portal** (available for VNC access method only): Record user activity on the web portal graphically.
  - **On Violation** (only valid if no other recording options are set): Start recording only when a user causes a violation against a Command Filter or Socket Filter during a session. The recording continues until the user ends the connection session.

#### NOTE

To view session recordings when accessed through a Juniper SA appliance, configure a policy for allowing custom headers. See [Junos configuration that is required for viewing session recordings](#).

12. If you are integrating with PAM Server Control, select **Login Integration** on the **PAM Server Control** tab. See [Privileged Access Manager Server Control Login Integration](#) for more information.
13. If you are using Transparent Login, select a **Login** on the **Transparent Login** tab. See [Device Setup, Transparent Login](#) for more information.
14. Optionally, set the **Extended Timeout** option on the **Timeout** tab to allow users who must run lengthy jobs (such as database backups) to specify a connection idle timeout longer than the default value. When extended timeout is enabled in an associated access policy, users are prompted to optionally specify a longer idle timeout (up to the new global **Maximum Connection Idle Timeout** setting) when starting an access session. This prevents such sessions from timing out (and the job in process abruptly terminated) if left unattended for longer than the global **Connection Idle Timeout** value (which is only 10 minutes by default). The maximum timeout that a user can request is defined by the global **Maximum Connection Idle Timeout** setting).

#### NOTE

For more information about global timeout settings associated with the extended timeout functionality, see the **Login Timeout**, **Connection Idle Timeout**, and **Maximum Connection Idle Timeout** entries in the [Global Settings](#).

15. Click **OK**. You return to the Policies list. The activated device or password access is now available for execution from the Access page of the user.

### **Junos Configuration Required for Viewing Session Recordings**

To view session recordings when Privileged Access Manager is accessed through a Juniper SA appliance, configure a policy for allowing custom headers.

#### **Follow these steps:**

1. Navigate to Resource Policies, Web, Custom Headers.
2. Create a policy.
3. Specify the IP address of the web portal resource that this policy applies to, with protocol specification, for example: `https://192.0.2.123 (IPv4)`, `https://[fd6d:8d64:af0c:1:0:242:22:233] (IPv6)`
4. Select the allow custom headers action.



**More information**

- [Import or Export Policies](#)
- [Set Up an AWS Policy](#)

**Import or Export Policies**

Instead of creating policies individually through the web interface, you can populate them into a comma-separated value (CSV) configuration file. The CSV file lets you load records for a batch of Users.

**Import a CSV Policy File**

A sample file is provided for spreadsheet editing and population.

**Download Sample CSV**

1. Go to **Policies, Manage Policies**.
2. Select the **Import/Export** button on the **Policies** page.  
The Import/Export Policies window appears.
3. Click **Download Sample File**.
4. Copy and rename the sample file, and open the new copy in any spreadsheet to inspect the column headers and cell values.  
Each line below the header is a full policy association.
5. Create and populate the new file. See [CSV Fields and Syntax](#) for details about each column.
6. In the Import/Export Policies window, click **Choose File** to locate your new file.
7. Click **Import Policy** to upload the CSV file.  
The imported policies are added to the Policies list.

**CSV Fields and Syntax**

Only the first three columns require a value. The order of the columns does not matter, but the spelling of their heading does, though they are not case-sensitive. Do not include empty columns (with no header).

- **Type:** Policy or SAML Service Policy  
SAML services are part of a policy, but they are imported in their own row:
  - A policy row deselects all SAML services for the specified policy. Therefore, if the policy row is not followed by SAML Service Policy (SSP) rows, all SAML services are deselected in the final policy.
  - SSP rows configure the specified SAML service only for the specified policy.
  - SSP rows that are not preceded by a policy row only update the SAML service configuration in the specified policy. It does not clear selected SAML services for the specified policy.
  - SSP rows depend on a preceding policy row or depend on the specified policy already existing. Attempting to import an SSP row without a policy results in an import error.
- **User:** User or User Group name of the User-Device pair.
- **Device:** Device Name or Device Group Name of the User-Device pair.
- **Services:** Specify built-in services (**sftpft**, **sftpftpemb**, **sftpstft**, **sftpstftpemb**, **TSWEB**) or custom Services. Separate multiple Services using a pipe character.  
For SAML Service Policy type rows, specify the name of the SAML service that is being configured.

Account information that is associated with these services can be specified by appending ',,, ' and using the following template to describe the account:

- **ts=DeviceName tap=TargetApplicationName tac=AccountName awsPolicyName=AWSPolicyName**
- *DeviceName* specifies the device name of the target account. This field is optional if the value is the same as the Device column. Specify this field only for the case where the account belongs to a credential source.
- *TargetApplicationName* specifies the name of the target application of the target account.
- *AccountName* specifies the account name of the target account.
- *AWSPolicyName* specifies the AWS policy that should be applied when this account is used. This field should only be specified for AWS accounts used with the special aws.amazon.com device.
- **Example:**  

```
TestService,,,ts=TestCredentialSourceDevice tap=TestApplication
tac=test_user,,,tap=TestAppBelongingToTestDevice tac=user1
```
- **Applets:** Use the following template for each Access Method applet: **name=Name custom\_name=CustomName**
  - *Name* options: **VNC, Telnet, SSH, SSH2, Telnet, RDP**
  - *Name* extra options if mainframe licensing is enabled: **TN3270, TN3270SSL, TN5250, TN5250SSL**
  - *CustomName* options: (empty); or any string
  - Separate any multiple applets (Access Methods) using a pipe character.

Account information that is associated with these applets can be specified by appending ',,, ' and using the following template to describe the account:

```
ts=DeviceName tap=TargetApplicationName tac=AccountName awsPolicyName=AWSPolicyName
```

  - *DeviceName* specifies the device name of the target account. This field is optional if the value is the same as the Device column. Specify this field only for the case where the specified account belongs to a credential source.
  - *TargetApplicationName* specifies the name of the target application of the target account.
  - *AccountName* specifies the account name of the target account.
  - *AWSPolicyName* specifies the AWS policy that should be applied when this account is used. This field should only be specified for AWS accounts used with the special aws.amazon.com device.
  - **Example:**  

```
name=SSH custom_name=OpenSSH,,,ts=TestCredentialSourceDevice tap=Active Directory
tac=Administrator,,,tap=TestAppBelongingToTestDevice tac=root
```

Multiple accounts can be associated with an applet by appending ',,, ' and more account descriptions as shown in the example.- **Command Filter:** If this policy uses one or more Command Filter Lists, enter them by name; otherwise, leave blank. If used, define CFLs (import CFL CSV file) first. Ensure that filters are imported before policy.
- **Socket Filter:** If this policy uses one or more Socket Filter Lists, enter them by name; otherwise, leave blank. If used, define SFLs (import SFL CSV file) first. Ensure that filters are imported before policy.
- **Restrict login if agent is not running:** Use "t" or "f" for true or false. Use this field only for applets that rely on this switch: RDP, VNC, and ICA.
- **Graphical Recording:** Use "t" or "f" for true or false. When true, CA PAM performs graphical recording of every RDP or VNC session between this User-Device (or Group) pair.
- **Command Line Recording:** Use "t" or "f" for true or false. When true, CA PAM performs command line recording of every CLI-based session between this User-Device (or Group) pair.
- **Bidirectional Recording:** Use "t" or "f" for true or false. When true (and Command Line Recording is true), CA PAM records the User and Device input for every CLI-based session between this User-Device (or Group) pair. Otherwise, only User input is recorded.
- **Web Portal Recording:** Use "t" or "f" for true or false. When true, CA PAM performs graphical recording of every web portal session between this User(Group)-Device(Group) pair.
- **Targets:** [**ts=deviceName**] **tap=targetApplicationName tac=accountName**
- **SAML Attributes:** | (pipe) delimited mapping of the attributes that are requested by the SAML service.  

```
name=(.*)\s+nameIdFormat=(.*)\s+provisionType=(.*)\s+xAttribute=(.*)\s+value=(.*)
```

SAML attributes should be on a row after a policy to which they apply, with SSP in the Type column. See **Type** for more information about the SAML Attribute column.

### **Export a CSV List of Policies**

To export existing policies to a CSV file:

1. Go to **Policies, Manage Policies**.
2. Select the **Import/Export** button on the **Policies** page.  
The Import/Export Policies window appears.
3. Select the **Export Policy** button.  
A CSV file is saved on your computer. The CSV file has the format of the sample file

### **Set Up an AWS Policy**

When a connection is made to AWS (Amazon Web Services), the **Manage AWS Policies** link interface is established for specifying an AWS IAM Policy. This policy is applied for AWS privileges when accessing the AWS management interface. To create an AWS policy, follow these steps:

1. Ensure that AWS is set up in **Configuration, 3rd Party, AWS**.
2. Select **Policies, Manage AWS Policies**.  
Two default policies are shown in the list. Edit these policies or create another IAM policy.
3. Enter values for each field, noting the following information:
  - **Access Key:** Lists the target accounts that are specified for use with the AWS Access Credential Accounts target application. Select the account whose credentials should be used to validate the AWS policy during save and update operations.
  - **Session Timeout** - Designates the amount of time that is permitted for the policy is applied before disconnection.
  - **Policy** - Shows the IAM policy content to be applied.

AWS does not accept a policy that is too lengthy. Privileged Access Manager sends all submitted policies to AWS for preprocessing so AWS can evaluate the length and avoid a disruptive error condition. If the policy exceeds the size limit, an error message is relayed to the user.

For guidance on permitted length, see this AWS Forum thread <https://forums.aws.amazon.com/thread.jspa?threadID=80882>

### **Use AWS Policies**

When a Service has been configured for access to the AWS management interface, the credential specification pop-up window in the Manage Policy interface also provides for the IAM policy specification through the **AWS Policy** field at the right-hand side of the pop-up window.

### **Dynamic Addition of Devices and Target Accounts to the Access Page Based on Target Group Membership**

Privileged Access Manager dynamically adds devices to the **Access** page if those devices are members a of a Credential Manager target group that is referenced by a Credential Manager user group to which the logged in user belongs.

If there is no policy for one of the devices in the group, PAM just allows the user to view the passwords for any credentials of the device from the **Access** page. If there is a policy for the device (either directly or via a device group) that has an applet or service that is attached then any relevant target accounts are added to the list of possible accounts for connection.

Devices are added to the **Access** page according to the following rules:

- If a user is not a Global (Super) Administrator or Operational Administrator,  
*and*
- The user belongs to a Credential Manager user group other than standard users that has the right to view passwords for some devices,  
*then:*
- The following logic is applied to each device and target account:
  - a. If there is an applet or service to which the target account can reasonably be assigned for autoconnect, that target account is assigned.
  - b. If not, the target account is available for viewing.

The mapping between target applications (each target account belongs to exactly one application) and applets/services is as follows:

- If a device has an SSH or Telnet applet, or an SSH or Telnet proxy service, any target account whose target application is either Generic or Unix will be assigned to it.
- If a device has an RDP applet, and RDP application, or an RDP Proxy service any target account whose target application is either Generic, Windows Proxy, or Active Directory will be assigned to it.
- If the device has a TN5250/TN5250 SSL applet a target application of either generic or AS400 will be assigned to it.
- Otherwise, if either the target account's target application is not one of the aforementioned types or if the device does not have the requisite applet or servlet assigned, the target account is available for viewing.

## Policy inspection

### View Policy

To view (and edit) explicitly assigned policy for a (User / User Group) and (Device / Device Group) pair, enter the policy editing mode.

### View Effective Policy

Without entering the policy editing mode, you can view a list of the current User or User Group effective policy across all individual Devices, directly from that User or User Group record. By "effective policy" is meant the combination of the policy that is:

- Explicitly set with each Device for that User or User Group
- Inherited from the policy of User Groups of which the current User is a member
- Inherited from the policy of Device Groups which are associated with the current User or User Group

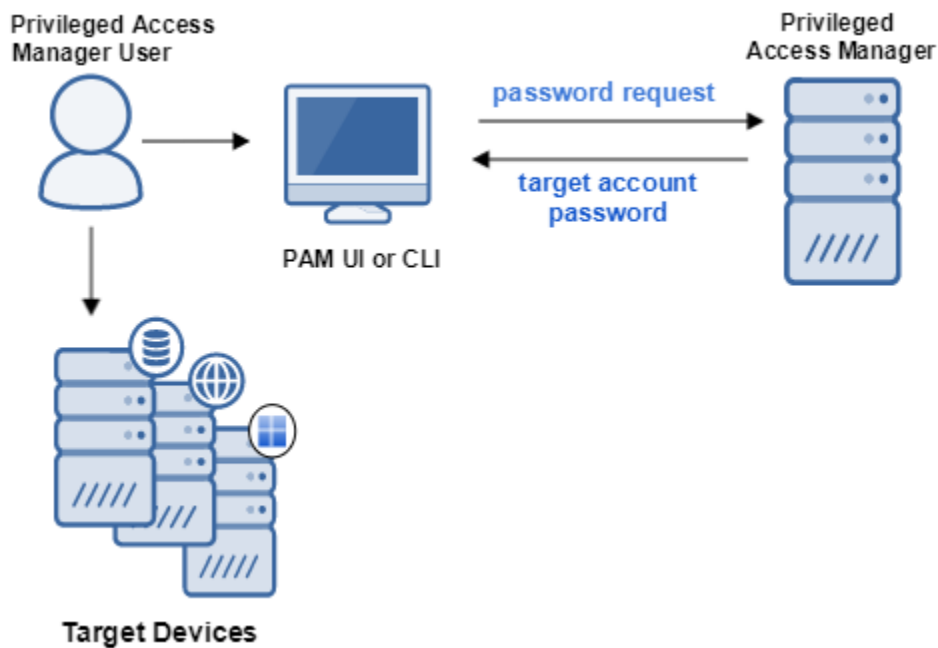
### **Procedure**

1. Open the **Users, Manage Users** page.
2. Move your mouse over a User record line item, and open it for editing by clicking it.
3. At the right-hand side of either the top or bottom of the User record, click the button **View Policy** .  
A shadow window appears with a list showing one Device record per line. Each Device displays its current access options (Access Methods, OOB, Services, SSLVPN, RDP Applications). Each Device record can be clicked to reveal, in a left pane, the actual policy pair generating the inheritance. By clicking **Expand All** or **Collapse All**, all records can be opened or closed, respectively.

## Implementing Credential Manager

Implement Credential Manager to protect privileged account credentials against a security breach. Privileged accounts have access to the most critical systems, services, and sensitive data so these types of accounts require secure management.

**Figure 22: Protecting Privileged Account Credentials**

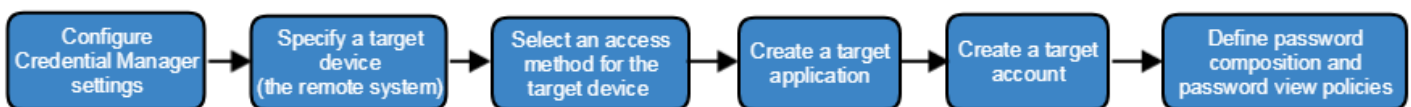


Credential Manager allows you to:

- Vault existing credentials
- Automatically roll over parts of those credentials
- Specify rules for generating new credentials
- Specify rules for viewing credentials, granting permissions to view credentials, and what action occurs after the password is viewed.

To protect a privileged account, you must configure several Credential Manager objects. The following graphic shows you, in order, the basic configuration tasks:

**Figure 23: Credential Manager Configuration Task Flow**



To use Credential Manager, become familiar with the following terms:

- **Target Server/Device**  
A device or *target server* is an application server that hosts one or more target applications that require access credentials. Device names must be unique.
- **Target Application**

The target application is a container for all managed accounts of a single application, such as all privileged users of an Oracle database. A target application can contain one or more target accounts. The target application also defines the connector, the mechanism for accessing target accounts. The connector allows for multiple applications or entities within the same server to contain the same account user name. For example, if a given server hosts two databases, each database is a unique target application. Each database could have a uniquely identified user account `dbasys`. Target application names must be unique within a given device.

- **Application Type/Target Connector**

The application type identifies the target connector. The target connector is the mechanism that lets Credential Manager manage and change credentials at a target. When you configure a target application, you select an application type—not a target connector—to identify the single application at the target server.

**NOTE**

The UI uses the term **application type**, not target connector. When you select an application type during target application setup, you are configuring the related target connector.

A predefined set of target applications are included with the appliance. For example, to connect to an Oracle database, configure the Oracle application type/target connector to update and verify passwords for Oracle target accounts.

- **Target Accounts**

The target account identifies an account at the remote server. The account specifies the set of credentials (for example, user name and password or user certificate). When you configure a target account, you identify a target application for that account. Target account user names must be unique for a given target application.

- **Target Aliases (for A2A deployments only)**

Aliases uniquely identify a specific target account. When an application requests credentials for another application, the requesting applications use the target alias. Target aliases eliminate the need to hard-code the name of the privileged account that has access to the target application.

## Default Ports for Credential Manager

The following tables list the ports that enable Credential Manager and associated target connectors use to communicate with each other. Ensure that networks and firewalls permit data transfer between these ports.

### Default Port Assignments for Credential Manager Components

You can configure the port number in the following file: `installation_directory/cspmclient/config/cspm_client_config.xml`.

**NOTE**

In the **Source** column, the term **Appliance** represents the Privileged Access Manager virtual or hardware appliance.

Default Port	Source	Destination	Name of Config Variable	Description
5900, 3306, 7900, 7901, 443	Appliance	Appliance	N/A	Communication between PAM appliances on the network.
27077	Appliance	Windows Proxy	Windows Proxy configuration file: <code>daemonserver_port</code>	PAM appliance to Windows Proxy communications
28088	A2A requesting application	A2A client daemon	A2A Client configuration file: <code>daemonserver1_port</code>	Used for A2A client stub requests. Daemon validates request is local.
28888	Appliance	A2A Client	A2A Client configuration file: <code>daemonserver2_port</code>	PAM Appliance to A2A Client host
443	A2A Client	Appliance	A2A Client configuration file: <code>cspmserver_port</code>	A2A Client to PAM Appliance

8550	Appliance	Server with Socket Filter Agent (SFA)	Socket Filter configuration file: port#	Leapfrog prevention and containment.
443	Socket Filter Agent	Appliance	N/A	Reporting policy violations

The appliance uses TCP port 5900. Network security scans typically assume that TCP port 5900 is used by a VNC server. For that reason, security scans might erroneously indicate that the appliance has a security vulnerability.

### Default Ports for Target Connectors

The following tables list the default ports that the out-of-the-box target connectors use to communicate with Credential Manager. Target connectors represent supported application types.

#### NOTE

In the **Source** column, the term **Appliance** represents the Privileged Access Manager virtual or hardware appliance.

If a target connector is not listed here, then firewall ports do not have to be open.

#### NOTE

For AWS or Azure, ensure that these ports are also open in the AWS or Azure network settings, and the OS firewall of the instance.

### Active Directory

Default Port	Source	Destination	Configurable	Applicability
636	Appliance	AD Domain Controllers	In the target application	
27077	Appliance	Windows Proxy	Windows Proxy configuration file: daemonserver1_port	For a target account configured to discover services or to discover scheduled tasks

### AS/400

Default Port	Source	Destination	Configurable	Applicability
449	Appliance	Target server	No	
8475	Appliance	Target server	No	
8476	Appliance	Target server	No	
9475	Appliance	Target server	No	Port must be open to use SSL

The AS/400 target connector uses the IBM Toolbox for Java and JTOpen. For details, see [https://www.ibm.com/support/pages/node/1119561?mhsrc=ibmsearch\\_a&mhq=ibm%20toolbox%20for%20java](https://www.ibm.com/support/pages/node/1119561?mhsrc=ibmsearch_a&mhq=ibm%20toolbox%20for%20java).

- Port 8475 provides Remote Command functionality (`as-rmtcmd`).
- Ports 449 and 8476 are for non-SSL services, such as AS/400 server mapping (`as-svrmap`) and AS/400 user ID and password validation (`as-signon`).

**AWS Access Credentials Accounts**

Default Port	Source	Destination	Configurable	Applicability
443	Appliance	iam.amazonaws.com	No	
443	Appliance	sts.amazonaws.com	No	AWS Policy

**Azure Active Directory**

Default Port	Source	Destination	Configurable	Applicability
443	Appliance	portal.azure.com	No	

**Cisco**

Default Port	Source	Destination	Configurable	Applicability
22	Appliance	Target server	In target application	If ssh is used
23	Appliance	Target server	In target application	If Telnet is used

**Juniper JUNOS**

Default Port	Source	Destination	Configurable	Applicability
22	Appliance	Target server	In target application	

**LDAP**

Default Port	Source	Destination	Configurable	Applicability
389	Appliance	LDAP server	In target application	

**MSSQL**

Default Port	Source	Destination	Configurable	Applicability
1433	Appliance	Microsoft SQL Server database host	In target application	

**MySQL**

Default Port	Source	Destination	Configurable	Applicability
3306	Appliance	MySQL server database host	In target application	

**Oracle**

Default Port	Source	Destination	Configurable	Applicability
1521	Appliance	Oracle server database host	In target application	



**SPML**

Default Port	Source	Destination	Configurable	Applicability
8080	Appliance	Target server	In target application	

**UNIX**

Default Port	Source	Destination	Configurable	Applicability
22	Appliance	Target server	In target application	If ssh is used
23	Appliance	Target server	In target application	If Telnet is used

**VMware ESX/ESXi**

Default Port	Source	Destination	Configurable	Applicability
443	Appliance	Target server	In target application	

**VMware NSX Controller**

Default Port	Source	Destination	Configurable	Applicability
22	Appliance	Target server	In target application	

**VMware NSX Manager**

Default Port	Source	Destination	Configurable	Applicability
22	Appliance	Target server	In target application	

**WebLogic 10**

Default Port	Source	Destination	Configurable	Applicability
7001	Appliance	Target server	In target application	

**Windows Proxy**

Default Port	Source	Destination	Configurable	Applicability
389, 636, 445	Windows Proxy Server	AD Domain Controllers	No	Domain accounts
389 and 636	Appliance	AD Domain Controllers	No	Domain accounts
27077	Appliance	Windows Proxy	Windows Proxy configuration file: daemonserver1_port	Sybase database communications
443	Windows Proxy Server	PAM appliance	No	Proxy requests
445	Windows Proxy Server	Target Servers	No	SMB2 communication

**Windows Remote**

Default Port	Source	Destination	Configurable	Applicability
445	Appliance	Windows target device	No	SMB2 communication

135	Appliance	Windows target device	No	WMI communication
49152 through 65535 1024 through 4999	Appliance	Windows target device	No	WMI communication

## Credential Manager Operation Settings

Before you configure credential management features, configure Credential Manager operational preferences.

### Specify General Operation Settings

The General Settings are preferences for Credential Manager operations.

To access these settings:

1. In the UI, navigate to **Settings, Credential Manager, General Settings**.
2. Configure the following preferences:
  - **Disable CLI Host Name Check**  
If a server is executing Credential Manager commands from the CLI, the server must provide a certificate to execute CLI commands. Select this option to override the verification of the appliance host name in the certificate.
  - **Allow Self Approval of Password View Request**  
Allows users who are authorized approvers to approve their own password view requests.
  - **Maximum Number of Report Entries**  
Sets the number of Credential Manager entries in a report. The default is 5000. We recommend that you limit entries to less than 5000 records. The maximum size ultimately depends on the type of report, its output format, and the available memory in Credential Manager. If an HTML report runs out of memory, try generating a CSV or a PDF file instead. Alternatively, use the `setReportRowLimit` CLI command.
  - **Password View Request Delete Interval Days**  
This checkbox specifies the number of days after which a password view request expires.  
**Example:** If you set this field to 12, the password view requests are deleted automatically from the My Approvals list when they become 12 days old. For information about the My Approval list, see [Credentials, Workflow, My Approvals](#).
  - **Automatically Update Expired Passwords**  
This checkbox enables automatic updates to the passwords for synchronized accounts when the password age exceeds the specification in its Password Composition Policy.
  - **Enable External CLI**  
This option enables the Credential Manager CLI. The CLI provides administrative access to password management functions, such as adding and modifying target and request data. The CLI also provides access to a limited set of maintenance operations. The Remote CLI is supported on UNIX, Linux, and Windows platforms. For more information, see [Use the Credential Manager CLI](#).
  - **Password View Request Banner**  
Optional. Enter the text for a banner that is displayed on Password View Requests. This banner can contain information about what users must enter in the Reason Description and Reference Code fields when viewing a password for an account. You can also set this banner on the Create a Basic Password View Policy page. If set as part of a Password View Policy, it takes priority over this General Setting.

### Archive and Purge Metrics and Audit Logs

Credential Manager produces many log messages in the form of metrics and audit logs. These logs are saved on your appliance and they can fill up your hard drive, which can be disastrous. These logs are not purged by the Automatic Log Purge feature, which only removes session logs. Use Auto-Archive to archive and purge these logs automatically. You configure archive settings for Metrics and Audit Logs separately. For more information about Metrics and Audit Logs, see [Credential Management Log Formats](#).

### **Prerequisite**

Archived logs are saved to a session recording mount, which must be set up first. See [Set Up Session Recording](#) for instructions.

#### NOTE

If you are using a Syslog server to save these messages, you can opt to purge and not archive them.

Follow these steps:

1. Select **Settings, Credential Manager** and select the **Auto-Archive** tab.  
Metrics and Audit Log archive settings are configured separately. Each section has the same fields.
2. Select an archive **Option**:
  - PURGE only. Do not archive.
  - Archive to PRIMARY Mount, then purge.
  - Archive to FAILOVER Mount, then purge.

#### NOTE

The Primary and Failover Mounts behave independent of their session recording purposes. Either mount can be used for either or both log types. The "Failover Mount" does not act as a failover for the Primary when archiving.

3. Select the log **Age (Days)** after which the purge or archive is performed. For example, to keep the most recent week of logs locally, select 7. The archive happens at midnight GMT and is not configurable.
4. To store the logs in a specific folder or folder path, enter it in the **Folder** field. If the folder does not exist, it is created by the process. The process appends a `server-id` folder and a `metrics-id` or `auditlogs-id` folder beneath your specified folder. The `id` is the Hardware ID found on the **Configuration, System Info, Hardware Identifiers** page. The full path appears as the **Storage** field value once the archive settings are saved successfully.
5. Select **Save**.

Once saved, the **Storage, Mount Status, and Mount Availability** states appear on the page.

#### Archive Process

Once an archive process has begun, status and statistics appear in the **Archive Process** area. Each cluster member has a row in Metrics and Audit Log, with the most recent information for that process.

The **Site** column lists the configured cluster site name, if any. The **IP Address** column is for the individual appliance or cluster member.

The options for **Status** are: Purge OK, Archive OK, Error, No Storage. If the status is "No Storage," the storage mount is not available, and the process deletes only non-essential logs. The **Status Date** denotes when the status shown was recorded.

The **Action Date** column is when the purge or archive was taken. This column can be empty if there was nothing to purge or archive during the most recent process.

Select the **Reset Process Statistics** button to clear the data.

Error messages and warnings are posted on the top of the [Dashboard](#) on the **Overview Tab**. To get rid of warnings on the **Dashboard Overview Tab**, select the **Reset Dashboard Warnings** button. This button is only active when there are warnings on the Dashboard.

#### Configure Settings for Request Servers

A2A credential management permits customer applications and scripts to obtain credentials for target applications. To use this feature, first configure settings for A2A request servers (which host A2A Clients). For more information about A2A Request Servers and A2A Clients, see [Configure A2A Credential Management](#).

Follow these steps:

1. Select **Settings, Credential Manager** and select the **Request Server Settings** tab.

**NOTE**

Some of the settings on the **Request Server Settings** tab apply to Credential Manager proxies.

2. Disregard the **A2A Global Settings**, which are currently not in use:
  - Check Execution User
  - Check Execution Path
  - Check File Path
  - Perform Script Integrity Validation
3. Review the **Request Server Global Settings**:
  - **FIPS 140-2 Mode**: Enables FIPS 140-2 mode for Credential Manager proxies.
  - **Preserve Client/Proxy Host Names**: Set this option to preserve the host name that PAM obtains (by performing a reverse DNS lookup) for an A2A client or proxy when it initially registers with PAM. If not set (the default), PAM repeats the reverse lookup and updates the initial hostname whenever a client or proxy does one of the following:
    - Restarts, triggering reregistration.
    - Requests credentials that result in a call to the PAM server
  - **Enable Hardware Fingerprinting**: Set this option to add a **Get Fingerprint** button to the **View A2A Client** dialog. Selecting the **Get Fingerprint** button obtains the latest **hardware fingerprint** from the **request server**. PAM uses **hardware fingerprints** to [uniquely identify a A2A Clients](#).
4. Select **Save**.

**Request Server Subnets**

The **Request Server Subnets** tab displays a list of auto-registered request server settings by subnet.

**To add a Request Server Subnet, follow these steps:**

1. Select **Add**.
2. In the **Add Request Server Subnet** dialog that opens, complete the fields:
3. Select **OK** to save your subnet.

**Configure Email Templates**

When a user views a password, an administrator or other user can receive an email notification. Email notifications are available only for password view policies. They are sent only for successful initial password view requests. Configure the email templates by selecting **Settings, Credential Management**, and then **Email Templates**. Configure the email server by selecting **Configuration**, and then **Email Settings**. After you specify these settings, then enable the notification in the password view policy. Notifications are configured on a per-policy basis.

To set up the email preferences, see [Email Preferences for Password View Policies](#).

To enable notifications, see [Enable Email Notification](#).

**Monitor Default Credential Manager Activities**

To help monitor Credential Manager activity, such as passwords not verified, create an activities list from a set of predefined metrics. You can add, remove, and reposition list items. You can set a threshold for the number of occurrences for a given activity to display a warning indicator in the list.

**Follow these steps:**

1. Select **Settings, Credential Manager, Default Activities List**.
2. To add an item to the list:
  - a. Select the **+** (plus) symbol. The Item Name window appears.
  - b. Select one or more items from the activity list.

- c. Select **OK**.

To reposition a list item, select the item and use the Up or the Down arrow.

To remove an entry from the Activities list, select the **X** icon.

3. To set a threshold limit that displays a warning icon in the list, enter an integer in the Threshold column. For example, enter a five for the Passwords Not Verified setting. When the number of unverified passwords reaches five, a warning icon appears in the Activities List page.
4. Select **Save**.

To display the activity report, select **Credentials, Reports, Activities**.

## Configure Email Preferences for Password View Policies

Email notifications are available for password view policies. When a user views an account password, an email is sent to other users who are configured to receive notifications. Emails are sent only for successful initial password view requests. For example, if the password is viewed for an already checked out account, no email is sent. To receive email notifications, configure the email server and default templates. If you enable dual authorization, authorization requests, approvals, and password views all trigger email notifications. The email contains text and links.

### To configure email notifications:

After the setup of email notifications is complete, you enable notifications in the password view policy, on a per-policy basis.

### Set Up the Email Server

To enable email notifications, first configure the connection between Credential Manager and the email server.

#### NOTE

The email server, application, and account must already be provisioned as targets in the database before the email template can be configured through the UI.

### Configure the Email Server from the UI

#### Follow these steps:

1. Select **Configuration, Email Settings**.
2. Optionally, select **Enable SMTP Server Authentication**.
3. If you selected the **Enable SMTP Server Authentication** option, the **Account Name** field appears. Use the magnifying glass to select your email account or type the email target account name.
4. If you selected **Enable SMTP Server Authentication** option, the **Host Name** field is automatically populated with the name of the target server. If you did not select the **Enable SMTP Server Authentication** option, or if the email server is different from the target server, edit the field as required.
5. Enter the **Port** number for the email server.
6. Optionally, select **Enable SMTP Server Debug**. This option helps diagnose email problems if you can also reproduce the issue, and then review the Tomcat logs under **Configuration > Diagnostic** for related information and errors.
7. In the **From Email Address** field, enter the email address to use.
8. Select **Enable TLS** to establish a secure connection using TLS.
9. Select the **Test** button to test to see if a sample email is sent to the user whose Email Settings you are configuring. A message appears indicating success or failure.

#### TIP

If the test was successful, the test email appears in the user's email in-box. If a message indicates failure, check the logs: Select **Configuration, Diagnostics, Diagnostic Logs**, the **Download** tab, and then the **Recent Log Entries** button to display the most-recent logs.

**NOTE**

This configuration is not applicable to Monitor (Legacy). See [Set Up Email for Monitoring \(Legacy\)](#) for more information.

**Configure the Email Server from the CLI**

To configure the email server from the CLI, use the `setSystemProperty` command to specify values for email server properties.

Use the following CLI command syntax and specify each email service property. The following example shows how to configure the `emailServerHost` property.

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailServerHost propertyValues=mail.yourdomain.com encryptValue=false
```

You can specify one or more of the properties in the following table, as required. Each property is separated by a space.

Property Name	Value	Required	Notes	encryptValue
<code>emailServerHost</code>	mail.yourdomain.com	Yes	Host name of the mail server	False
<code>emailServerPort</code>	Port number	No	Port number the SMTP service is listening on. Default is 25.	False
<code>emailTransportType</code>	smtp or smtps	No	Email transport type. Default: <code>smtp</code> . Selecting the <code>smtps</code> type allows you to use the TLS email transport type.	False
<code>emailTargetAccount</code>	Target account ID	No	Target account ID of the email setting	False
<code>oneclickServerHost</code>	mail.yourdomain.com	Yes	Credential Manager Primary Host name	False
<code>emailFromAddress</code>	view_requests@yourdomain.com	Yes	The "From" address for emails	False

**Modify Email Templates**

Credential Manager supplies default templates for the following types of email:

- [Request email](#)
- [Request status email](#)
- [Retrospective approval request email](#)
- [Password view email](#)
- [Expired password view request email](#)
- [One-click approval email](#)
- [Report results email](#)

These tasks can be completed from the UI or from the CLI, using the command `setSystemProperty`.

To customize the content of email notifications, modify the default email templates. Each template is explained in this topic. You can modify the email settings in the UI or with the CLI command `setSystemProperty`.

All email templates contain tokens. When Credential Manager generates an email, it uses the tokens in the email templates to look up request-specific items. Credential Manager populates the tokens at runtime. The tokens are case-sensitive and use the following syntax: @ClassName.methodName@

Each template is described in the following subsections. The values of *ClassName* and *methodName* vary depending on the type of email.

### **Request Email Configuration**

A request email is sent from a requestor to list of approvers.

#### **Configure the Request Email Template from the UI**

**Follow these steps:**

1. Select **Settings, Credential Manager**, and then the **Email Templates** tab.
2. Modify the template text for the Request Subject and Request Body as desired.  
For the request email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getDeviceName getHostName
PasswordViewPolicy	getName
PasswordViewRequest	getReason getReasonDescription getSsoType getReferenceCode getConnectionTimeout
User (the user name generating the password view request)	getUserID getFirstName getLastName getEmail

#### **Configure the Request Email Template from the CLI**

**Follow these steps:**

1. Specify the first property for the request email template:  

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailRequestBody propertyValues="Do not reply to this email.
A password view request has been submitted by user @User.getUserID@ to view the
password for account @TargetAccount.getUserName@ of application
@TargetApplication.getName@ on server @TargetServer.getHostName@.
The password view request reason is @PasswordViewRequest.getReason@
(@PasswordViewRequest.getReasonDescription@). Please login to the CPA
system and manage this request."
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailRequestBody	Do not reply to this email. A password view request has been submitted by user @User.getUserID@ to view the password for account @TargetAccount.getUserName@ of application @TargetApplication.getName@ on server @TargetServer.getHostName@. The password view request reason is @PasswordViewRequest.getReason@ (@PasswordViewRequest.getReasonDescription@). Please log in to the CPA system and manage this request.	No
emailRequestSubject	Password View Request for target account @TargetAccount.getUserName@	No

### **Request Status Email Configuration**

The request status email is sent from an approver to a requestor. This notification informs the requestor whether the request was approved or denied.

### **Configure the Request Status Email Template from the UI**

Follow these steps:

1. Select **Settings, Credential Manager**, and then the **Email Templates** tab.
2. Modify the template text for the **Request Status Update Subject** and **Request Status Update Body** as desired. For the request status email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getDeviceName getHostName
PasswordViewPolicy	getName
PasswordViewRequest	getStatusString getSsoType getApprovalReason getApprovalReasonDescription getReferenceCode getConnectionTimeout
User (the approver of the password view request)	getUserID getFirstName getLastName getEmail

### **Configure the Request Status Email Template from the CLI**

Follow these steps:

1. Specify the first property for the request status email template:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
```



```
propertyName=emailRequestStatusBody propertyValues="Do not reply to this email.
The status of your request to view password for the account @TargetAccount.getUserName@
of application @TargetApplication.getName@ in server @TargetServer.getHostName@, is:
@PasswordViewRequest.getStatusString@."
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailRequestStatusBody	Do not reply to this email. The status of your request to view password for the account @TargetAccount.getUserName@ of application @TargetApplication.getName@ in server @TargetServer.getHostName@, is: @PasswordViewRequest.getStatusString@.	No
emailRequestStatusSubject	Password View Request Status for account @TargetAccount.getUserName@	No

### ***Retrospective Approval Email Configuration***

Retrospective approval email is sent to an approver. This notification informs the approver that a user has requested immediate emergency "break glass" access to account credentials.

### **Configure the Retrospective Approval Request Email Template from the UI**

Follow these steps:

1. Select **Settings, Credential Manager**, and then the **Email Templates** tab.
2. Modify the template text for the **Retrospective Approval Request Subject** and **Retrospective Approval Request Body** as desired.  
For the retrospective approval email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getDeviceName getHostName
PasswordViewPolicy	getName
PasswordViewRequest	getStatusString getSsoType getApprovalReason getApprovalReasonDescription getReferenceCode getConnectionTimeout
User (the approver of the password view request)	getUserID getFirstName getLastName getEmail

### **Configure the Retrospective Approval Request Email Template from the CLI**

**Follow these steps:**

1. Specify the first property for the retrospective approval email template. For example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailRetrospectiveApprovalRequestSubject propertyValues="Password View
Request for target account @TargetAccount.getUserName@"
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailRetrospectiveApprovalRequestBody	@TargetApplication.getName@ in server @TargetServer.getHostName@ with device name @TargetServer.getDeviceName@ has been submitted by user @User.getUserID@. This is a retrospective approval request. Please login to Privileged Access Manager system and manage this request.	No
emailRetrospectiveApprovalRequestSubject	Password View Request for target account @TargetAccount.getUserName@	No

Retrospective approval email is sent to an approver. This notification informs the approver that a user has requested immediate emergency "break glass" access to account credentials when the **Enable One Click Approval** option is enabled in the password view policy.

**Password View Email Configuration**

A password view email is sent from a user to a set of users when a password is viewed. This section describes how to configure the password view email through the template.

**Configure the Password View Email Template from the UI****Follow these steps:**

1. Select **Settings, Credential Manager**, and the **Email Templates** tab.
2. Modify the template text for the Password View Subject and Password View Body as desired.  
For the password view email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getHostName getDeviceName
PasswordViewPolicy	getName
PasswordViewRequest	getSsoType getReason getReasonDescription getReferenceCode getConnectionTimeout

User (the user name viewing the password)	getUserID getFirstName getLastName getEmail
--	--

### **Configure the Password View Email Template from the CLI**

#### **Follow these steps:**

1. Specify the first property for the password view email template:

```
capam_command adminUserID=admin capam=mycompany.com
cmdName=setSystemProperty propertyName=emailPasswordViewBody
propertyValues="Do not reply to this email. The Password for the account
@TargetAccount.getUserName@ of application @TargetApplication.getName@ on
server @TargetServer.getHostName@ has been accessed by user @User.getUserID@."
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailPasswordViewBody	Do not reply to this email. The Password for the account @TargetAccount.getUserName@ of application @TargetApplication.getName@ on server @TargetServer.getHostName@ has been accessed by user @User.getUserID@.	No
emailPasswordViewSubject	Password of account @TargetAccount.getUserName@ has been accessed by @User.getUserID@	No

### ***Expired Password View Request Email Configuration***

An approver who is expiring the request sends the expired password view request email to a requestor. The email is also sent to any other approvers in dual authorization list. The email is auto-generated when a request in Pending/Approved status expires.

### **Configure the Expired Password View Template from the UI**

#### **Follow these steps:**

1. Select **Settings, Credential Manager**, and then the **Email Templates** tab.
2. Modify the template text for the Expired Password View Request Subject and Expired Password View Request Body as desired.  
For the expired password view request email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getHostName getDeviceName
PasswordViewPolicy	getName

PasswordViewRequest	getSsoType getReferenceCode
User (the user name generating the password view request)	getUserID getFirstName getLastName getEmail

### **Configure the Expired Password View Template from the CLI**

#### **Follow these steps:**

1. Specify the first property for the expired password view request email template:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailExpiredPasswordViewRequestBody
propertyValues=" Do not reply to this email. The Password View Request
for the account @TargetAccount.getUserName@ of application
@TargetApplication.getName@ on server @TargetServer.getHostName@
requested by user @User.getUserID@ has expired."
```

2. Repeat the previous step for each property as required. Refer to the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getHostName
PasswordViewPolicy	getName
PasswordViewRequest	getReason getReasonDescription getStartDate getEndDate getReferenceCode getConnectionTimeout
User (user who is generating the password view request)	getUserID getFirstName getLastName getEmail

### **One Click Approval Email Setup**

A one-click approval email is sent from a requestor to a list of approvers.

#### ***Configure the One Click Approval Email Template from the UI***

#### **Follow these steps:**

1. Select **Settings, Credential Manager**, and then the **Email Templates** tab.
2. In the **One Click Approval Server Host Name** field, enter the Credential Manager server host name that you use in the approve or deny URL. The URLs are sent in the email whenever the request for viewing the account password with enabled one-click approval, is generated.

**NOTE**

By default, the primary site host name is used. Admin is authorized to edit this name.

3. Modify the template text for the One Click Approval Subject and One Click Approval Body as desired.  
For the one-click approval email, @ClassName.methodName@ tokens can have the value pairs that are shown in the following table.

ClassName Values	methodName Values
TargetAccount	getUserName
TargetApplication	getName getType getExtensionType
TargetServer	getHostName getDeviceName
PasswordViewPolicy	getName
PasswordViewRequest	getReason getReasonDescription getStartDate getEndDate getSsoType getReferenceCode getConnectionTimeout
User (user who is generating the password view request)	getUserID getFirstName getLastName getEmail

The one-click approval email template also contains following specialized tokens:

- @PasswordViewRequestIdentifier.getApprovalUrl@ - Use this token to show the URL to approve the password view request.
- @PasswordViewRequestIdentifier.getDenialUrl@ - Use this token to show the URL to deny the password view request.

### ***Configure the One Click Approval Email Template from the CLI***

#### **Follow these steps:**

1. Specify the first property for the one click approval email template:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailOne Click ApprovalBody propertyValues=" Do not reply to this email.
<br><br>A password view request has been submitted with the following details:
<br>Requestor: @User.getUserID@<br> Requested Account: @TargetAccount.getUserName@
<br> Requested Account Target Application Name: @TargetApplication.getName@
<br> Requested Account Target Server: @TargetServer.getHostName@
<br> Request Reason: @PasswordViewRequest.getReason@
(@PasswordViewRequest.getReasonDescription@)
<br>Start Date: @PasswordViewRequest.getStartDate@
<br>End Date: @PasswordViewRequest.getEndDate@<br>
<br><a href='@ApprovalURL@'>Click here to Approve this Request</a><br>
<br><a href='@DenialURL@'>Click here to Deny this Request</a>."
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailOneClickApprovalBody	Do not reply to this email.   A password view request has been submitted with the following details:  Requestor: @User.getUserID@   Requested Account: @TargetAccount.getUserName@   Requested Account Target Application Name: @TargetApplication.getName@   Requested Account Target Server: @TargetServer.getHost@   Request Reason: @PasswordViewRequest.getReason@ (@PasswordViewRequest.getReasonDescription@) Start Date: @PasswordViewRequest.getStartDate@  End Date: @PasswordViewRequest.getEndDate@   <a href='@ApprovalURL@ '>Click here to Approve this Request</a>  <a href='@DenialURL@ '>Click here to Deny this Request</a>	No
emailOneClickApprovalSubject	Password View Request for target account @TargetAccount.getUserName@	No

### **Report Results Email Configuration**

The report results email is sent from a requestor to a list of approvers.

### **Configure the External Retrospective Approval Request Email Template from the UI**

Follow these steps:

1. Select **Settings, Credential Manager**, and then the **Email Settings** tab.
2. Modify the template text for the Report Results Subject and Report Results Body as desired.

The report results email template contains following specialized tokens:

- @reportName@ - Use this token to show the report name.
- @reportStartDate@ - Use this token to show the "From" date of the report results.
- @reportEndDate@ - Use this token to show the "To" date of the report results.

### **Configure the Report Results Email Template from the CLI**

Follow these steps:

1. Specify the first property for the report results email template:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=emailReportResultsBody propertyValues=" Do not reply to this email.
The @reportName@ report has been run. The attached results encompass the period from
@reportStartDate@ to @reportEndDate@."
```

2. Repeat the previous step for each property as required. Refer to the following table.

Property Name	Default Value	Required
emailReportResultsBody	Do not reply to this email. The @reportName@ report has been run. The attached results encompass the period from @reportStartDate@ to @reportEndDate@ .	No
emailReportResultsSubject	Report results for @reportName@	No

## Secrets Expiration Notification Email Configuration

The secrets expiration notification email is sent to all users with the SecretOwners or VaultOwners permissions when a secret is about to expire. Users with a custom role receive the email if they have the updateSecret privilege. The email is sent daily starting at the number of days before expiration that you set in the **Secret Expiration Threshold (Days)** field.

### Configure the Secrets Expiration Notification Email Template from the UI

Follow these steps:

1. Select **Settings, Credential Manager**, and then the **Email Settings** tab.
2. Click the **Notify of Upcoming Secret Expirations** option to enable the notification email. No emails are sent unless this option is enabled.
3. Modify the template text for the secrets expiration notification email as desired.

The secrets expiration notification email template contains following specialized tokens:

- @reportName@ - Use this token to show the report name.
- @Secret.getVaultName@ - Use this token to show the name of the vault in which the expiring secret is stored.
- @Secret.getName@ - Use this token to show the name of the expiring secret.
- @Secret.getAutoExpireDate@ - Use this token to show the date that the secret expires.

### Configure the Secrets Expiration Notification Email Template from the CLI

Follow these steps:

1. Specify the emailSecretExpirationBody property for the Secrets Expiration Notification email template:

```
capam_command adminUserID=super capam=10.17.44.202 cmdName=setSystemProperty
propertyName=emailSecretExpirationBody "propertyValues=The following secrets are about to expire
or be deleted: <table width=\"800\" cellspacing=\"1\" bgcolor=\"#000000\"><tr bgcolor=\"#ffffff
\"><th>Vault Name</th><th>Secret Name</th><th>Expiration Date</th></tr>@<tr bgcolor=\"#ffffff\"><td
align=\"center\">@Secret.getVaultName@</td><td align=\"center\">@Secret.getName@</td><td align=\"center
\">@Secret.getAutoExpireDate@</td></tr>@</table> Please log in to PAM for more information about these
secrets."
```

Property Name	Default Value	Required
emailSecretExpirationBody	The following secrets are about to expire or be deleted: <table width="800" cellspacing="1" bgcolor="#000000"><tr bgcolor="#ffffff"><th>Vault Name</th><th>Secret Name</th><th>Expiration Date</th></tr>@<tr bgcolor="#ffffff"><td align="center">@Secret.getVaultName@ </td><td align="center">@Secret.getName@ </td><td align="center">@Secret.getAutoExpireDate@ </td></tr>@</table> Please log in to PAM for more information about these secrets.	Yes

## Specify a Target Server

After you configure the Credential Manager settings, identify the target servers, which host the target applications.

### Add a Target Server Using the UI

To identify a target server in the UI:

1. In the UI, select **Devices, Manages Devices**.
2. From the **Devices** page, select **Add**.
3. In the **Add Device** dialog, complete the required fields in the **Basic Info** tab.

4. For the **Device Type**, select the **Password Management** check box.
5. Go to the **Access Methods** tab and specify an access protocol. The appliance uses the access method to contact the remote target server.
6. Select **OK** to complete the configuration.

### **Add a Target Server using the CLI**

To add a target server using the CLI, use the command `addTargetServer`.

The following command examples show how to add a target server using the CLI.

#### **NOTE**

Any literal IPv6 address entered in the `Address` field will be normalized according to the following standard:  
[RFC 5952: A Recommendation for IPv6 Address Text Representation](#).

For example, entering `1111:2222:000A:000B:0:0:0:D` in the `Address` field, and then saving it, means this value converts to `1111:2222:a:b::d`, enforcing the lowercased and compressed value according to the RFC 5952 standard.

Windows example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 ^
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

Linux example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 \
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

## **Identify Target Applications and Connectors**

Credential Manager protects remote applications by associating specific user accounts with the applications. You then apply password policies for these accounts.

The following graphic shows the relationship between the target application, the target connector, and the target account. The value of the `Application Type` field determines the target connector and its relevant settings. The target account is then associated with the application. Multiple target accounts can be associated with a single target application.



**Figure 24: PAM App, Connector, Account**

The diagram illustrates the configuration of a PAM application, connector, and account. It consists of three windows:

- Add Target Application (Left):**
  - Application: MySQL
  - Host Name: 123.22.23.4
  - Device Name: mylinux
  - Application Name: SQL1
  - Application Type: MySQL
  - Password Composition Policy: (empty)
  - Descriptor 1: (empty)
  - Descriptor 2: (empty)
- Add Target Application (Right):**
  - Application: MySQL
  - DB Port: (empty)
- Add Target Account (Bottom):**
  - Account: Password Compound Servers MySQL
  - Host Name: 123.22.23.4
  - Device Name: mylinux
  - Application Name: SQL1
  - Account Name: root
  - Account Type: Privileged Account
  - Access Type: (empty)
  - Descriptor 1: (empty)
  - Descriptor 2: (empty)

Arrows indicate the following relationships:

- A green arrow points from the **Application Name** field in the left **Add Target Application** window to the **Application Name** field in the **Add Target Account** window.
- A blue arrow points from the **Application Type** field in the left **Add Target Application** window to the **Application** field in the **Add Target Account** window.
- A blue arrow points from the **DB Port** field in the right **Add Target Application** window to the **Application** field in the left **Add Target Application** window.

### Application Types and Target Connectors

An application type corresponds to a third-party operating system, database, directory, or other application that is remote to Privileged Access Manager. These target applications contain privileged accounts that are protected by passwords, cryptographic keys, and other mechanisms. Credential Manager manages these applications using target connectors.

The target application type has a one-to-one relationship to the target connector, which enables Credential Manager to communicate with the remote target application. When you specify an application type, you are configuring the associated target connector.

Target applications can contain one or more target accounts. The applications are grouped by the server where they are hosted, known as the target server. A target server can contain one or more target applications.

### Out-of-the-Box Application Types

Each out-of-the-box application type has a related target connector that enables Credential Manager to communicate with remote target application. After you select an application type, the related tabs for the associated target connector display in the Add Target Application dialog. Configure the target connector by completing the configuration settings.

#### NOTE

The UI uses the term **application type** not target connector.

### List of Out-of-the-Box Application Types

Credential Manager currently provides out-of-the-box target connectors for the following applications:

- Generic
- Active Directory
- Active Directory SSH Key
- AWS Proxy Access Credentials
- AWS Access Credentials
- Azure AD
- Azure Access Credentials
- BMC Remedy
- CA NIM
- Cisco
- HP Service Manager
- IBM i
- Juniper Junos
- LDAP
- MSSQL
- MSSQL Azure Managed Instance
- MYSQL
- Oracle
- Palo Alto
- RADIUS/TACACS+
- ServiceNow
- SPML
- UNIX
- VMware ESX/ESXi
- VMware NSX Controller
- VMware NSX Manager
- VMware NSX Proxy
- WebLogic
- Windows SSH Key
- Windows SSH Password
- Windows Remote
- Windows Proxy
- API Key

***See Out-of-the-Box Application Types in the UI***

To see the list of out-of-the-box application types in the UI:

1. Log in to the UI.
2. Select **Credentials, Manage Targets, Applications**.
3. Select **Add**.
4. In the **Application Type** field, look at the drop-down list to see all the options.

**Custom Application Types and Target Connectors**

If the out-of-the-box application types and target connectors are not sufficient for your remote applications, you can build custom target connectors. A Custom Connector framework is available for Privileged Access Manager. This framework provides the necessary components to deploy a target connector framework and the required APIs to build custom target connectors.

The target connector framework and the custom target connectors enable password viewing and password changes to your remote target system.

For information about how to deploy the software and build a custom target connector, see [Add a Custom Target Connector](#).

### **Target Connector Configuration**

After you select an application type, a new tab for the target connector displays. This tab has the configuration settings for the connector. For fields descriptions of each connector, select the relevant connector from the Table of Contents in the left pane.

## **Add an Active Directory Target Connector**

The Active Directory connector, Windows Proxy connector, and Windows Remote connector all manage Windows accounts. Use the Active Directory connector to update the passwords of Active Directory accounts. This connector uses the LDAPS interface to Active Directory to update account passwords. If the connector communicates with a deployed Windows Proxy or a Windows Remote connector, you can use this connector to update Windows services and scheduled tasks.

The Active Directory target connector performs the following activities:

- Verifies and synchronizes the password against an Active Directory database
- Queries one or more DNS servers to find domain controllers (optional)
- Uses LDAPS to connect to the domain controller
- If you use a domain account for a service or for a scheduled task, one or more Windows Proxies update the credentials and restart services.
- Uses HTTPS and AES encryption for secure communications.

To add the target connector using the CLI, see [Active Directory CLI Configuration](#).

To add the target connector using the external API, see [Active Directory Target Connector External API Configuration](#).

### **Add the Target Application and Connector**

Follow these steps in the PAM UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name**: Select the magnifying glass to pick the target server.
  - **Device Name**
  - **Application Name**: Application names must be unique for a given target server.
4. In the **Application Type** field, select **Active Directory**.
5. (Optional) Select a password composition policy.

#### **NOTE**

If you do not select a password composition policy, a default policy is used. This policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.

6. On the **Active Directory** tab, configure the following fields:
  - **Domain Controller Lookup**: Specify the DNS method to identify the domain controller:

- **Do not use DNS (target server is domain controller):** Use the target server as the domain controller.
- **Retrieve DNS list:** Use the first reachable DNS server that is configured in the [PAM server network settings](#) to look up the domain controller.
- **Use the following DNS server:** Specify the IP address or (comma-separated) addresses of one or more DNS servers to use to look up the domain controller. If there are multiple entries, PAM uses the first reachable DNS server in the list to look up the domain controller.
- **Domain Name:** Specifies the Windows domain to which accounts managed by this application are members.
- **Domain Controller Port (SSL):** Specify the port that is used to connect to the Domain Controller. The default is 636. If the LDAPS port is the default 636, this field can be left blank. Otherwise, the port must be populated. Port 389 is used for unencrypted LDAP. Credential Manager does not synchronize AD target accounts using unencrypted LDAP
- **Active Directory Site:** This field is used only if **Domain Controller Lookup** is set to **Retrieve DNS list** or **Use following DNS server**.
  - If a value is given, the connector uses the value to narrow the search for domain controllers.
  - If empty, the connector searches for all domain controllers in the DNS.
- **Use Kerberos:** (Optional) Set this option to enable authentication using the Kerberos protocol. The name of the Kerberos realm is displayed in the **Realm Name** field that appears.

**NOTE**

Kerberos verifies user identities using a Key Distribution Center (KDC), which is a service that runs on Windows domain controllers. PAM uses the KDC on the domain controller which is determined by the previously configured **Domain Controller Lookup** setting.

7. If you enabled [Account Discovery](#), also complete the following settings:
  - **Groups:** To limit the number of discovered accounts, specify one or more comma-separated Active Directory groups. Do not use the Active Directory Primary Group for Account Discovery. Account Discovery does not find users in the Primary Group.
  - **Active Directory Connect Timeout:** enter the timeout for connecting to the directory in milliseconds. The default is 3000.
  - **Active Directory Read Timeout:** enter the timeout for reading from the directory, in milliseconds. The default is 3000.
8. If you are using target groupings, provide descriptors for the target application.
9. Select **OK**.

**NOTE**

Next Step: [Add a target account to the target application](#).

## Active Directory Target CLI Configuration

This topic includes CLI commands and parameters for adding Active Directory target applications and target accounts.

### Active Directory Target Connector CLI Parameters

To add an Active Directory target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	windowsDomainService

**Attribute.disableAutoConnectTargetAccount**

Disable automatic connections to the remote target server for all target accounts using this application type.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>true - disables automatic connectivity. Automatic connections are not allowed.</li> <li>false - enables automatic connectivity. Automatic connections are allowed.</li> </ul>

**Attribute.domainName**

The Windows domain that is managed by the Active Directory Server.

Required	Default Value	Valid Values
yes	N/A	Domain name (text string)

**Attribute.enableKerberos**

Determines whether Kerberos authentication is enabled for a target application.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>true - Kerberos authentication is enabled.</li> <li>false - Kerberos authentication is not enabled.</li> </ul>

**Attribute.useDNS**

Determines the level to which DNS is used.

Required	Default Value	Valid Values
yes	none	<ul style="list-style-type: none"> <li>noDNS. DNS is not used</li> <li>retrieveDNS. Retrieve the DNS server that is used by the Credential Manager server</li> <li>specifiedDNS. Use the DNS server that is specified by the dnsServer attribute</li> </ul>

**Attribute.dnsServer**

The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if Attribute.useDNS is set to specifiedDNS	none	Comma separated list of DNS server host names.

**Attribute.dcPort**

The port that is used to connect to the Active Directory server.

Required	Default Value	Valid Values
no	636	Numeric

**Attribute.adSite**

The Active Directory site. This parameter is only used if `Attribute.useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers based on the specified name.

Required	Default Value	Valid Values
no	N/A	String

**Active Directory Target Account CLI Parameters**

To add an Active Directory target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

**Attribute.extensionType**

Specifies the type of account to be used.

Required	Default Value	Valid Values
yes	N/A	windowsDomainService

**Attribute.userDN**

The users distinguished name on the Active Directory Server.

Required	Default Value	Valid Values
yes	N/A	String.

**Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.otherAccount**

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
Required if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	String. A valid target account ID.

**Attribute.serviceInfo**

List of services.

Required	Default Value	Valid Values
No	N/A	<p>&lt;empty string&gt; no services</p> <p>Add <i>one</i> of the following entries for each service:</p> <ul style="list-style-type: none"> <li>• &lt;proxy_hostname&gt;:&lt;hostname&gt;:&lt;service_name&gt;</li> <li>• &lt;proxy_hostname&gt;:&lt;hostname&gt;:&lt;service_name&gt;</li> </ul> <p>Multiple services are delimited by the   character.</p> <p>&lt;proxy_hostname&gt; is the name of the server running the proxy.</p> <p>&lt;hostname&gt; is the name of the server where the service is hosted.</p>

### ***Attribute.tasks***

List of scheduled tasks.

Required	Default Value	Valid Values
No	none	<p>&lt;empty string&gt; no tasks</p> <p>Add the following for each task:</p> <p>&lt;proxy_hostname&gt;:&lt;hostname&gt;:&lt;task_name&gt;</p> <p>Multiple tasks are delimited by the   character.</p> <p>&lt;proxy_hostname&gt; is the name of the server running the proxy.</p> <p>&lt;hostname&gt; is the name of the server where the scheduled task is hosted.</p>

### **Active Directory CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myAD TargetApplication.type=windowsDomainService
Attribute.domainName=cspm2
```

```
Attribute.useDNS= specifiedDNS Attribute.dnsServer=dns1.cloakware.com,dns2.cloakware.com
```

```
Attribute.dcPort=636 Attribute.adSite=London
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=mywindows
```

```
TargetAccount.userName=admin TargetAccount.password=P@ssw0rd
TargetAccount.cacheAllow=true
```

```
TargetAccount.cacheDuration=19 Attribute.extensionType=windowsDomainService
Attribute.useOtherAccountToChangePassword=false
```

```
Attribute.forcePasswordChange=false Attribute.userDN=cn=admin,dc=cspm2
```

```
Attribute.serviceInfo=proxyhostA:HostA:serviceName:restart|
proxyhostB:HostB:serviceName:norestart
```

```
Attribute.tasks=proxyHostA:HostA:taskName|proxyHostB:HostB:taskName
```

## Active Directory Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating Active Directory target applications using the External API.

### Active Directory Target Application External API Attributes

To add or update an Active Directory target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call.

#### ***disableAutoConnectTargetAccount***

Disable automatic connections to the remote target server for all target accounts using this application type.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>true - disables automatic connectivity. Automatic connections are not allowed.</li> <li>false - enables automatic connectivity. Automatic connections are allowed.</li> </ul>

#### ***domainName***

The Windows domain that is managed by the Active Directory Server.

Required	Default Value	Valid Values
yes	N/A	Domain name (text string)

#### ***useDNS***

Determines the level to which DNS is used.

Required	Default Value	Valid Values
yes	none	<ul style="list-style-type: none"> <li>noDNS. DNS is not used</li> <li>retrieveDNS. Retrieve the DNS server that is used by the Credential Manager server</li> <li>specifiedDNS. Use the DNS server that is specified by the dnsServer attribute</li> </ul>

#### ***dnsServer***



The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if <code>useDNS</code> is set to <code>specifiedDNS</code>	none	Comma separated list of DNS server host names.

### ***dcPort***

The port that is used to connect to the Active Directory server.

Required	Default Value	Valid Values
no	636	Numeric

### ***adSite***

The Active Directory site. This parameter is only used if `useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers based on the specified name.

Required	Default Value	Valid Values
no	N/A	String

### ***enableKerberos***

Determines whether Kerberos authentication is enabled for a target application.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>true - Kerberos authentication is enabled.</li> <li>false - Kerberos authentication is not enabled.</li> </ul>

### **Active Directory External API Example**

```
{
  "applicationName": "My Sample AD",
  "applicationType": "windowsDomainService",
  "attributes": {
    "domainName": "mydomain",
    "useDNS": "specifiedDNS",
    "dnsServer": "dns1.mydomain.com",
    "dcPort": "636",
    "adSite": "Boston"
  },
  "description1": "Sample AD Target App created from the External API"
}
```

## Add an Active Directory SSH Key Target Connector

Key authentication has long been recognized as providing a higher level of security than passwords when connecting to Linux/Unix devices over SSH. Key authentication suffers from two limitations:

- The user public key must be stored in the `Authorized_keys` file on the target device
- The user must protect the private key with a passphrase to prevent compromising all the target systems where that key-pair has access.

Rather than managing key pairs for many users on many devices, Symantec PAM can manage access to and the lifecycle of a key pair specific to each target system. This management ensures users only access the private key through PAM after authentication and authorization, making governance and audit simpler to administer. This approach still requires a public key to be held in the target system's `Authorized_keys` file, although the attack surface is greatly reduced and access control is centralized.

The Active Directory SSH Key Target connector supports managing a `sshKey` in Active Directory as an attribute of the Active Directory user. This functionality allows a PAM user to SSH into a Linux system, and then be authenticated using a public key stored in an Active Directory system.

This connector allows you to use PAM to manage the lifecycle of the Keypair, providing an automated solution using Active Directory-backed target accounts for Linux systems, without making any changes to the servers, and allowing credential rotation policies to work. This feature will provide a AD/LDAP connector where the secret is public key generated and managed by PAM and the target is a Unix or Linux device.

Configuring this connector requires the following sections:

### **1. Create a Device in PAM for the Active Directory System**

Create a device in PAM to represent the Active Directory system that will contain the credentials used to access the PAM Linux devices you want users to access. Follow the directions as described in the [Device Setup](#) topic.

### **2. Create an Active Directory SSH Key Target Application for the Active Directory Device**

This step requires that you create an Active Directory SSH Key target application for the Active Directory device. You must specify the attribute name where the public key will be stored.

The default attribute name is `sshPublicKeys`.

**Follow these steps:**

1. Log in to the UI.
2. Select **Credentials, Manage Targets**, and then **Applications**. The **Target Applications** screen appears.
3. Select **Add**.
4. Complete the fields as described in the [Add Target Accounts to Target Applications](#) topic, with the following modifications:
5. In the **Application Type** option, use the drop-down list to select **Active Directory SSH Key**. Selecting **Active Directory SSH Key** displays a new tab labeled **Active Directory SSH Key**.
6. In the **SSH Key Attribute Name** field, enter the name of the attribute in Active Directory where the actual public key is stored. The default is `sshPublicKeys`. However, the names must match.
7. In the **SSH Key Pair Policy** field, select the search icon (magnifying glass) to display the **SSH Key Pair Policies** window. The key pair policy controls the attributes of certain attributes of the key when generated by PAM.
8. Select the desired key pair policy, and then select **OK**. If left blank, the default policy is RSA with a key length of 2,048. For more information on SSH key pair policies, see [SSH Key Authentication for Accessing UNIX/LINUX Targets](#).
9. Select **OK** to create the application.

### **3. Create an Active Directory Target Application for the Active Directory Device.**

Create an Active Directory target application for the Active Directory device. Follow the steps in the [Add an Active Directory Target Connector](#) topic. You must create a target application for the Active Directory device to allow PAM to store public keys in Active Directory. This target application is a prerequisite to creating a target account with sufficient privileges to update the attribute (default name **sshPublicKeys**) of the user account.

### **4. Create a PAM Target Account for the Active Directory Target Application.**

This step creates a PAM target account that represents the Active Directory account that PAM uses to connect to Active Directory and update the attribute.

#### **NOTE**

This user account must have sufficient privileges to update the SSH Key attribute.

Follow the steps in the [Add Target Accounts to Target Applications](#) topic.

### **5. Create a PAM Target Account for the Active Directory SSH Key Target Application.**

The private key is stored as the PAM password, and the public key is updated in Active Directory. The PAM target account is an account of the Active Directory device.

Section 2 creates the application, and this step creates the PAM account. There will be a corresponding account with this name on the UNIX target system the user is trying to access.

You use the following account to change the public key stored in the attribute: The Active Directory account credentials used to connect to and write into Active Directory.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets**, and then **Accounts**. The **Target Accounts** screen appears.
2. Select **Add**.
3. Complete the fields as described in the [Add Target Accounts to Target Applications](#) topic, with the following modifications:
4. Select the **Search** icon next to the **Application Name** field to display the list of target applications.
5. Select the application you created in [Step 2: Create an Active Directory SSH Key Target Application for the Active Directory Device](#), and then select **OK**. Making this selection populates the **Host Name**, **Device Name**, **Password View Policy**, and **Account Type** fields. Key options also appear on the right-hand side of the screen.
6. In the **Account Name** field, enter the name of an account that exists in both the Active Directory (as a user account) and UNIX systems.
7. Do *one* of the following tasks:
  - For the appliance to generate the key pair, select the keys icon next to the **Private Key** box.
  - To upload keys that are generated by a utility, select **Choose File** next to the Private and Public key boxes. Browse to the relevant file on your local system.
8. Select the **Password** tab. In the **Synchronized** setting, select **Update both the Credential Manager Server and the target system**.
9. Select the **Active Directory SSH Key** tab. You will select the Active Directory Account built in step 4. This is the account that is used to connect to AD and update the attribute.
10. Select the magnifying glass **Search** icon next to the **Use the following account to change the password** field to display the **Target Accounts** screen. The accounts table is populated by any account for that host and for the Active Directory type.
11. Create target accounts for every UNIX account you want users to log into using the credentials in Active Directory
12. Select **OK**, and both the PAM database and Active Directory synchronize

## **6. Create PAM Devices for the Linux-PAM End Targets with SSH Access.**

In this step, create PAM devices for the Linux-PAM end targets that have SSH access.

Follow the directions as described in the [Device Setup](#) topic, paying special attention to the [Specify Access Methods](#) subtopic, to make sure the devices use SSH.

## **7. Create a Device Group Containing Linux-PAM Devices with a Credential Source that is the Active Directory System with SSH Access.**

In this section, you create a device group, pick the device to include in the device group, and then select the Active Directory device as the credential source to associate with the group.

### **Follow these steps:**

1. Complete the fields as described in the [Device Group Setup](#) topic, with the following modifications:
2. Select the **Basic Info** tab.
3. From the list of devices under **Available Credential Source**, use the shuttle controls to select the Active Directory device as the **Selected Credential Source**.
4. Select the **Devices** tab.
5. Select the device to associate with this credential source.
6. Select **OK** to confirm your choices.

## **8. Create a Policy for a PAM User for the Device Group Granting SSH Access to the Active Directory SSH Key Target Account.**

In this section, you create a policy that grants SSH access to the Active Directory SSH Key target account for a PAM user for the device group created in section 7.

### **Follow these steps:**

1. Select **Policies, Manage Policies**, and then **Add**.
2. Complete the fields as described in the [Set Up a Policy](#) topic, with the following modifications:
3. In the **Add Policy** screen, use the **Device Group** option to select the device group created in section 7.
4. Select the **Access** tab to grant SSH access and associate the required target accounts to which you want to allow access:
5. Select **SSH** from the list and move it to the **Selected Access** list.
6. Select the magnifying glass **Search** icon in the corresponding **Target Account** column to display the **SSH Access** screen. This screen lists the target accounts that can get SSH access, including the UNIX accounts the user wants to be able to access.
7. Use the shuttle to select the Selected Target Account.
8. Select **OK** to confirm your choices.

## **Active Directory SSH Key Target CLI Configuration**

Learn how to use CLI commands and parameters for adding and updating Active Directory SSH Key target applications and target accounts.

This topic includes CLI commands and parameters for adding and updating Active Directory SSH Key target applications and target accounts, as well as example command strings.

### **Active Directory SSH Key Target Connector CLI Parameters**

#### ***Add or Update Active Directory SSH Key Target Application***

To add an Active Directory SSH Key target application and connector using the CLI, use the `addTargetApplication` command and its parameters.

To update an Active Directory SSH Key target application using the CLI, use the `updateTargetApplication` command and its parameters.

Both add and update operations use the `keyattribute` parameter to specify the attribute name where to store the public key. The default attribute name is `sshPublicKeys`.

### ***Add or Update Active Directory SSH Key Target Account***

To add an Active Directory SSH Key Target Account using the CLI, use the `addTargetAccount` command and its parameters.

To update an Active Directory SSH Key Target Account using the CLI, use the `updateTargetAccount` command and its parameters.

You can also use the following parameters:

- **anotherAccount:** The account ID of the PAM Active Directory Administrator target account. This is an Administrator account on the Active Directory that is used to connect to Active Directory and update the `keyattribute` parameter.
- **passwordViewPolicyId:** The ID of the PAM password view policy that is assigned to the target account.

### **Active Directory SSH Key CLI Examples**

#### ***CLI to Add an Active Directory SSH Key Target Application***

```
capam_command capam=capamServer adminUserID=admin cmdName=addTargetApplication
TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=ActiveDirectorySSHKeyApp
TargetApplication.type=activeDirectorySshKey
Attribute.keyattribute="sshPublicKeys"
Attribute.descriptor1="sample"
```

#### ***CLI to Update an Active Directory SSH Key Target Application***

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetApplication
TargetServer.ID=7001 TargetApplication.name=adSSHkey
TargetApplication.type=activeDirectorySshKey
TargetApplication.ID=11001 Attribute.keyattribute="sshPublicKeys"
Attribute.descriptor1="updated"
```

#### ***CLI to Add an Active Directory SSH Key Target Account***

```
capam_command.bat capam=capamServer adminUserId=admin
cmdName=addTargetAccount
TargetServer.hostName=myhostname.mydomain.com
TargetApplication.ID=9001
TargetAccount.userName=johnSmith
TargetAccount.passwordViewPolicyId=1000
TargetAccount.privileged=true
TargetAccount.synchronize=true
Attribute.anotherAccount=34001
Attribute.protocol=SSH2_PUBLIC_KEY_AUTH
TargetAccount.password="_generate_pass_"
```

## CLI to Update an Active Directory SSH Key Target Account

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetAccount
TargetAccount.ID=49001
TargetServer.hostName=myhostname.mydomain.com
TargetApplication.ID=11001
TargetAccount.userName=johnSmith
TargetAccount.passwordViewPolicyId=1000
TargetAccount.privileged=true
TargetAccount.synchronize=true
Attribute.anotherAccount=34001
Attribute.protocol=SSH2_PUBLIC_KEY_AUTH
TargetAccount.password="_generate_pass_"
```

## Active Directory SSH Key Target Application External API Attributes

This topic describes the required and supported Attributes used when adding or updating Active Directory SSH key target applications using the External API.

### Active Directory Target Application External API Attributes for Applications

To add or update an Active Directory target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call.

#### keyattribute

In Active Directory, the attribute name where the public key will be stored. The default attribute name is sshPublicKeys.

Required	Default Value	Valid Values
yes	sshPublicKeys	alphanumeric string

### Active Directory Target Application External API Attributes for Accounts

To add or update an Active Directory target account using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call.

#### anotherAccount

The account ID of the PAM Active Directory Administrator target account. This is an Administrator account on the Active Directory used to connect to the Active Directory and update the keyattribute.

Required	Default Value	Valid Values
yes	no	numeric string

**protocol:SSH2\_PUBLIC\_KEY\_AUTH**

SSH2\_PUBLIC\_KEY\_AUTH indicates that the target account will use SSH Public Key authentication

Required	Default Value	Valid Values
yes	SSH2_PUBLIC_KEY_AUTH	SSH2_PUBLIC_KEY_AUTH

**REST Web Service External API Examples****Add an Active Directory SSH Key Target Application**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "ADSSHKeyApp",
  "applicationType": "activeDirectorySshKey",
  "attributes": {"keyattribute": "sshPublicKeys"},
  "description1": "sample description1",
  "description2": "sample description2"
}
```

**Update an Active Directory SSH Key Target Application**

```
PUT /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "id": "11001",
  "applicationName": "adSSHkey",
  "applicationType": "activeDirectorySshKey",
  "attributes": {"keyattribute": "sshPublicKeys"},
  "description1": "updated"
}
```

**Add an Active Directory SSH Key Target Account**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts
{
  "accountName": "johnSmith",
  "attributes": {
    "anotherAccount": "34001",
    "protocol": "SSH2_PUBLIC_KEY_AUTH"
  },
  "password": "_generate_pass_",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "t"
}
```

### **Update an Active Directory SSH Key Target Account**

```
PUT /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountId":"49001",
  "attributes":{
    "anotherAccount":"39001",
    "protocol":"SSH2_PUBLIC_KEY_AUTH"
  },
  "password":"_generate_pass_",
  "passwordViewPolicyId":1000,
  "privileged":"t",
  "synchronize":"t"
}
```

## **Add an AWS Access Credentials Target Connector**

The AWS Access Credentials target connector provides a placeholder application for Amazon Web Services (AWS) access credentials. The connector can be associated only with the built-in target server `xceedium.aws.amazon.com`

### **NOTE**

This connector is available only when Privileged Access Manager is licensed for AWS capability.

### **View the Target Application and Connector**

The AWS Access Credentials application type is pre-configured in the UI. To add the connector using the CLI, see [AWS Access Credential CLI Configuration](#).

#### **To view the settings:**

1. Select Credentials, Manage Targets, Applications.
2. Select Update. The default settings are shown:
  - Host Name: `xceedium.aws.amazon.com`
  - Device Name: `xceedium.aws.amazon.com`
  - Application Name: AWS Access Credential Accounts
  - Application Type: `AwsAccessCredentials`
3. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. This policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
4. Select **OK**.

### **Add an AWS Access Credentials Target Account**

Follow the standard steps for adding target accounts, but add accounts only for AWS access.

For the **AWS Access Credential Type** setting, you have two options. Complete the other fields for the option you select:

- Access key
- EC2 Private key

#### **Access Key Fields**



- **User Friendly Account Name:** Enter a string that functions like a username for AWS Account + Region access.
- **Access Key ID:** Specify an alphabetic string that functions in AWS like a username for AWS account access.
- **Secret Access Key:** Enter the longer string corresponding to the Access Key ID that functions like a password with the above ID.
- **View Private Key:** Select this checkbox to reveal the Secret Access Key characters (which are otherwise obfuscated).
- **Key Alias:** Assign a short name to this credential pair for easy identification. Other fields in the UI may require you select this alias.
- **Access Role Name:** If these credentials are applicable to an AWS API Proxy account, provide this parameter.
- **AWS Cloud Type:** Select one of the following options:
  - Commercial if these credentials are applicable to a regular AWS account.
  - Government if applicable to a United States government authorized AWS GovCloud (US) Region account.

### EC2 Private Key Fields

- **EC2 Instance User Name:** For most AWS Linux instances, this parameter is pre-assigned: “ec2-user”.
- **EC2 Private Key:** Displays the private key file after you upload it using the select File and Upload buttons.
- **Upload Key File:** Select the \*.pem file you downloaded while creating the key pair in the AWS interface. Upload this file into the **EC2 Private Key** field.
- **Enable Key Upload:** Select this checkbox to activate the select File and Upload buttons.
- **Passphrase:** If you assigned a passphrase when creating the EC2 private key, enter it here. Select **Show Passphrase** to see the passphrase characters.
- **Key Pair Name:** Assign a short name to this credential pair for easy identification. Other fields in the UI may require you select this alias.

### NOTE

Next Step: [Add a target account to the target application.](#)

## AWS Access Credentials CLI Configuration

You can add an AWS Access Credentials target application and connector using the CLI. This topic contains the parameters for target applications and target accounts:

### AWS Access Credentials Target Application CLI Parameters

To add a target application that uses the AWS Access credentials, use the [addTargetApplication](#) command and the following parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	AwsAccessCredentials

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	AwsAccessCredentials

**AWS Access Credentials Target Account CLI Parameters**

To add a target account that uses the AWS Access Credentials, use the [addTargetAccount](#) command and the following command parameters:

***Attribute.awsCredentialType***

The AWS access credential type.

Required	Default Value	Valid Values
yes	EC2_PRIVATE_KEY	<ul style="list-style-type: none"> <li>SECRET_ACCESS_KEY</li> <li>EC2_PRIVATE_KEY</li> </ul> X509_CERT_PRIVATE_KEY and CLOUDFRONT_PRIVATE_KEY are not supported.

***Attribute.passphrase***

The EC2 key passphrase.

Required	Default Value	Valid Values
no	N/A	A string consisting of alphanumeric characters (a-z, A-Z, 0-9)

***Attribute.awsKeyPairName***

The EC2 key pair name.

Required	Default Value	Valid Values
Yes when credential type is EC2_PRIVATE_KEY	N/A	A string consisting of any character except @

***Attribute.accountFriendlyName***

**NOTE:** This attribute is deprecated. See **Attribute.awsAccessKeyAlias**. The access key user-friendly name.

Required	Default Value	Valid Values
Yes when credential type is SECRET_ACCESS_KEY	N/A	A user-friendly account name string

***Attribute.awsAccessKeyAlias***

The access key user-friendly name.

Required	Default Value	Valid Values
Yes when credential type is SECRET_ACCESS_KEY	N/A	A user-friendly account name string

***Attribute.awsAccessRole***

The user defined AWS access role.

Optional	Default Value	Valid Values
When credential type is SECRET_ACCESS_KEY	N/A	A string of up to 64 alphanumeric characters. The string can also include '+=, @-'

### ***Attribute.awsCloudType***

The AWS cloud environment type.

Required	Default Value	Valid Values
yes when credential type is SECRET_ACCESS_KEY	commercial	<ul style="list-style-type: none"> <li>commercial</li> <li>government</li> </ul>

### **AWS Access Credentials CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com

TargetApplication.name=My_AWS_Access_Credentials
TargetApplication.type=AwsAccessCredentials
Attribute.extensionType=AwsAccessCredentials cmdName=addTargetAccount

TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=My_AWS_Access_Credentials
TargetAccount.userName=admin TargetAccount.password=ASJKNSKKA9FJJSFS
Attribute.extensionType=AwsAccessCredentials Attribute.awsMasterAccount=1001
Attribute.awsCredentialType=SECRET_ACCESS_KEY Attribute.accountFriendlyName=xceediumAWS
Attribute.awsAccessRole=Admin Attribute.awsCloudType=commercial
```

## **Add an Azure AD Target Connector**

Use the Azure Active Directory (AD) connector to update the passwords of Azure AD accounts. This connector can only manage Azure AD accounts, not any other accounts included in the Azure portal.

### **IMPORTANT**

The Azure AD target connector does not require that the PAM server is also running on Azure. However, if the PAM server is not running on Azure, the network firewall where the PAM server is running must permit data transfer over port 443 to access portal.azure.com over the internet.

### **TIP**

The Azure AD target connector does not support temporary passwords assigned to Azure AD user accounts when an Active Directory administrator creates a new account or changes the password of an existing user from within Azure. Users with such temporary passwords must log in to the Azure portal using the temporary password and change it to a permanent one before the Azure AD target connector can handle that user account.

### **Create the Application in Azure**

The Azure Application allows Privileged Access Manager to access Azure Resource Groups, VMs (for Azure device import), network interfaces, and public IPs (for clustering).

**NOTE**

For clustering, configure the Azure Application on the first Primary Site member. See [Set Up a Cluster](#) and [Cluster Deployment Requirements for Azure](#) for more information.

To create an Application in Azure, follow these steps:

1. In Azure, select **Azure Active Directory** from the left menu.
2. Select **App Registrations** from the resulting service list.
3. Select **+New Registration** on the resulting pane.
4. Enter a **Name** of your choice. Do not include spaces in the name.
5. Select **Supported Account Types**: Accounts in this organizational directory only
6. Select **Public client (mobile & desktop)** for **Redirect URI**.
7. Enter a **Redirect URI** for the application. Use your Privileged Access Manager URL. For example: `https://ip_address/cspm/home` For a cluster, select the IP address of the first node at the primary site.
8. Select **Register**. The application is created and its property page appears.
9. Under **Call APIs**, select **View API Permissions**.
10. On the API Permissions panel, select **Microsoft Graph**.
11. Select **Delegated permissions**.
12. Under **Select permissions**, type to search for "directory."
13. In the search results, select **Directory.AccessAsUser.All** (Access directory as the signed in user).
14. Select **Update Permissions**.
15. Under **Grant consent**, select **Grant admin consent for [your directory]**.
16. Close **Request API permissions**.

**NOTE**

When troubleshooting, ensure that the Azure application permissions are correct and intact.

17. On the application menu, select **Authentication**.
18. Locate the **Advanced Settings** section, and enable the **Allow public client flows** setting by selecting the **Yes** option.
19. Select **Save**.
20. Select **Overview** from the application menu.
21. Copy the **Application (client) ID** and the **Directory (tenant) ID** for use in creating a Privileged Access Manager Target Account.

Now, associate your Application to your Resource Group:

1. Select **Resource Groups** from the Azure left menu.
2. Select your Resource Group.
3. Select **Access Control (IAM)**.
4. Select **+Add, Role Assignment**.
5. Select **Contributor** from the **Role** drop-down list. Leave **Assign Access to** as "Azure AD user, group, or service principal."
6. In the **Select** field, enter the name of your application. Select the application from the resulting list.
7. Select **Save**.

**NOTE**

If you run several PAM server instances in different Azure Resource Groups (such as for clustering), repeat this association for each Resource Group.

## Create a Target Account

Managing Azure AD accounts, Clustering, Azure device import, and the Azure agent require a Target Account in Privileged Access Manager.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. Use the **Application Name** magnifying glass icon to search and select **Azure Access Credential Accounts**. This action populates **Host Name** and **Device Name** with `ca.portal.azure.com`.
4. Select the **Key** tab.
5. Select the **Discovery Allowed** check box.
6. Select the **Update both the Credential Manager Server and the target system** radio button.
7. Select the **Access Credential** tab.
8. For **Azure Application Type**, select **Native Client**. A Native Client requires a user name and password.
9. For **User Name**, enter your Azure User Name.
10. For **Password**, enter your Azure Password. Do not use Generate Password for the account you use for discovery. Only Azure Global Administrators or Password Administrators can change their own passwords through Privileged Access Manager. Other users must use an administrator account as their master account.
11. Enter the **Application ID** from your Azure Application. If you did not copy it earlier, follow these steps:
  - a. In Azure, select **More Services** from the bottom of the left menu.
  - b. Enter "enterprise" in the filter field, and select **Enterprise Applications**.
  - c. Select **All Applications** from the menu.
  - d. Select your application from the application list.
  - e. Select **Properties**.
  - f. Copy the **Application ID** GUID from the property page.
12. Get the **Directory ID** from Azure. Follow these steps:
  - a. In Azure, select **Azure Active Directory** from the left menu.
  - b. Select **Properties** from its menu.
  - c. Select the **Directory ID** GUID from its property page.
13. Accept or change any other fields as appropriate.
14. Select **OK** to save the Target Account.

### IMPORTANT

If you are using the Azure SQL Managed Instance for JIT Provisioning, **stop here**. Do not do Step 15.

15. Follow the instructions in [Use Account Discovery to Add Target Accounts](#) to discover Azure Active Directory accounts using this target account. The account must be a Global Administrator for discovery.

### NOTE

Azure passwords expire independently of Privileged Access Manager. For this reason, you should configure Privileged Access Manager to rotate your Azure AD passwords more frequently than your Azure deployment does.

## Add a BMC Remedy Target Connector

The Remedy Target Connector helps you communicate with BMC Remedy Service Desk software.

For all the steps necessary to configure integration with BMC Remedy, see [BMC Remedy ITSM Integration](#).

## Add CA NIM Target Connectors

CA Normalized Integration Management (CA NIM) lets the Privileged Access Manager integrate with third-party service desk solutions. The appliance has two pre-existing target applications you can configure:

- CA NIM UM for User Management
- CA NIM SM for Service Management

For information about configuring CA NIM connectors, go to [Integrate with Your Service Desk Solution](#).

## Add a Cisco Target Connector

Use the Cisco connector to manage accounts on a Cisco router or switch. This connector uses either the SSHv2 or Telnet protocol for communication. The connector does not support SSHv1.

To add the target connector using the CLI, see [Cisco Target Connector CLI Configuration](#).

To add the target connector using the CLI, see [Cisco Target Connector External API Configuration](#).

### Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name:** Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name:** Application names must be unique for a given target server.
4. In the **Application Type** field, select **Cisco**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. This policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select the tab for the access communication method you are using (SSH-2 or Telenet) and fill-in the required fields.

#### **SSH-2 Tab - Connection information**

- **Port:** Enter the port that connects to the Cisco host using SSH.
- **Communication Timeout:** Specify the amount of time the appliance waits for communication from the remote target server before ending the connection.
- **Enable strict host key checking:** Select this checkbox to control whether a system with an unknown or changed host key gets automatically added to the known host list. Provide the Known Host Key or the Known Host Key Fingerprint so the host can be verified

#### **SSH-2 Tabs - Cipher, Hash, Key Exchange, Compression, Server Host Key**

Selecting the checkbox on each tab results in the appliance using the supported settings for each feature. Clearing the checkbox displays more settings, letting you customize how the appliance handles the SSH-2 features.

- **Cipher:** Select the checkbox to use supported ciphers. Clear the checkbox to reveal fields for entering a list of inbound and outbound ciphers.
- **Hash:** Specifies whether the supported hashes should be used when making an SSH connection to the remote host. Clear the checkbox to reveal fields for entering a list of inbound and outbound hashes.
- **Key Exchange:** Select the checkbox to use supported key exchange methods. Clear the checkbox to reveal fields for entering a list of key exchange methods.
- **Compression:** Select the checkbox to use supported compression methods. Clear the checkbox to reveal fields for entering a list of inbound and outbound compression methods.
- **Server Host Key:** Select the checkbox to use supported server host key types. Clear the checkbox to reveal fields for entering a list of server host key types.

#### NOTE

Encryption standards continue to evolve with new vulnerabilities identified in what were previously accepted algorithms. Progress is also made with additional more-secure Cipher, Hash, Key Exchange, or Server Host Key options added to common utilities used for establishing secure communication channels. When upgrading PAM, be sure to consider any changes in the available more-secure cipher algorithms. Less secure Ciphers, Hashes, Key Exchanges, or Server Host Keys algorithms are not listed, but will continue working but may be subject to removal in a future release.

#### 7. Telnet Tab

- **Port:** Enter the port that the appliance uses to connect to the UNIX host with Telnet. Default: 23
- **Communication Timeout:** Specify the amount of time, in milliseconds, that the appliance waits for communication from the remote target server. When this interval ends, the appliance terminates the connection. Default: 60000

#### 8. Select **OK**.

#### Use a Script to Simplify Communication (Optional)

The Cisco target connector includes a large amount of low-level code to handle communications with the remote host. Credential Manager can use a script processor to simplify such communications.

The script processor (written in Java) executes a high-level version of the logic for manipulating credentials on remote hosts. Two scripts allow different levels of testing and production use. One script verifies passwords while the other script updates passwords.

A set of default scripts that is provided with the appliance. To use the default scripts, configure a set of default prompts and command values.

When adding target applications and target accounts, you can configure the script settings with the UI or the CLI.

#### ***Generate the Script***

#### **Follow these steps to generate the script in the UI:**

1. Select the **Script Processor** tab.
2. Complete the following fields
  - Cisco Variant: Select the version of Cisco IOS software you are using.
  - Script Timeout (optional): Enter the amount of time, from 5000 through 59999 milliseconds, that the appliance waits to receive expected input from the remote host. Default: 5000

When specified, the following prompts and commands are substituted into appropriate locations (variables) in the default scripts. You can enter a substitute string.

- **Password Change Prompt:** A regular expression that matches the remote host prompt when it requests that a password be changed because it has expired.  
Default: (?si).\*?change your password.\*?
- **Password Confirmation Prompt:** A regular expression that matches the remote host prompt when it requests a password confirmation.

Default: (?si).\*?password:.\*?

- **Password Entry Prompt:** A regular expression that matches the remote host prompt when it requests a password.

Default: (?si) (. .\*?password(\sfor|:). .\*?)

- **User Name Entry Prompt:** A regular expression that matches the remote host prompt when it requests a user name. Default: (?si). .\*?login:.\*?

### ***Apply the Script to Update and Verify Credentials***

#### **Follow these steps:**

1. Select the **Credentials Script** tab.
2. In the Update and Verify sections, select one of the available options:

#### **TIP**

We recommend that you use the default script. If a revised script is required, contact CA Services.

- **Use the default script**  
Select this option for the appliance to use the default script that is provided with the release. If changes to the script logic are required, contact CA Services.
- **Use a revised default script (requires patch)**  
Select this option to use a revised script that is provided by CA Services. Select the appropriate script from the drop-down list.
- **Use a replacement script**  
Select this option to use a replacement script. When selected, this option opens the **Replacement Script** text box. Paste the new script in the box, and try the operation.  
You might have to try more than one replacement script so the appliance conforms to your OS environment. Only edit the replacement scripts with assistance from CA Services.

#### **WARNING**

**Customer Responsibilities for Custom Scripts:** If you build custom scripts, you are responsible for the operation between the target application and the target endpoint. CA Technologies is responsible for operation up to the point where PAM passes information to the custom target application. After that point, you are responsible for how the custom script handles communication at an operational and security level.

#### **NOTE**

**Next Step:** [Add a target account to the target application](#)

## **Cisco Target CLI Configuration**

This topic includes CLI commands and parameters for adding Cisco target applications and target accounts.

### **Cisco Target Application CLI Parameters**

To add a Cisco target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	CiscoSSH

#### ***Attribute.sshPort***



The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### ***Attribute.sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.sshStrictHostKeyCheckingEnabled***

Enables or disables strict host key checking. When enabled, Credential Manager compares the public key that is received from the remote host when making a connection to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Required	Default Value	Valid Values
no	false	true, false

#### ***Attribute.sshKnownHostKey***

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

#### ***Attribute.sshKnownHostKeyFingerprint***

Contains the fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is used for display purposes only to allow the user to compare one key with another. The fingerprint that is specified must correspond to the specified public host key.

Required	Default Value	Valid Values
no	N/A	a public key fingerprint

#### ***Attribute.sshUseDefaultCiphers***

Specifies whether the default ciphers should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerToClientCiphersList***

Specifies the list of ciphers to accept on the inbound data stream from the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

#### ***Attribute.sshClientToServerCiphersList***

Specifies the list of ciphers to use on the outbound data stream to the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

#### ***Attribute.sshDetectCiphersList***

Specifies the list of ciphers to detect when connecting to the remote host. Credential Manager does not attempt to use ciphers that are unavailable even if they are specified to use as inbound and outbound ciphers. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

#### ***Attribute.sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerToClientHashesList***

Specifies the list of hashes to accept on the inbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

**Attribute.sshClientToServerHashesList**

Specifies the list of hashes to accept on the outbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

**Attribute.sshUseDefaultKeyExchangeAlgorithms**

Specifies whether to use the default key exchange methods when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**Attribute.sshKeyExchangeAlgorithmsList**

Specifies the list of key exchange methods to use when connecting to the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultKeyExchangeAlgorithms</code> is false	diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1	A comma-separated list containing one or more of the following values: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1. Do not use spaces in the list.

**Attribute.sshUseDefaultCompressionAlgorithms**

Specifies whether the default compression methods should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**Attribute.sshServerToClientCompressionAlgorithmsList**

Specifies the list of compression methods to accept on the inbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A (do not use compression)	comma-separated list containing one or more of the following values: zlib, zlib@openssh.com. Do not use spaces in the list.

**Attribute.sshClientToServerCompressionAlgorithmsList**

Specifies the list of compression methods to use on the outbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
Yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A (do not use compression)	A comma-separated list containing one or more of the following values: <code>zlib</code> , <code>zlib@openssh.com</code> . Do not use spaces in the list.

#### ***Attribute.sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerHostKeyAlgorithmsList***

Specifies the list of host key types to accept when Credential Manager connects to the remote host.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultServerHostKeyAlgorithms</code> is false	<code>ssh-rsa,ssh-dss</code>	A comma-separated list containing one or more of the following values: <code>ssh-rsa</code> , <code>ssh-dss</code> . Do not use spaces in the list.

#### ***Attribute.telnetSessionTimeout***

When using the Telnet communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.telnetPort***

The port that is used to connect to the UNIX host using Telnet.

Required	Default Value	Valid Values
no	23	0-65536

#### ***Attribute.ciscoVariant***

Specifies the type of Cisco system that is installed on the target server.

Required	Default Value	Valid Values
no	<code>IOS_12_4</code>	<code>IOS_10_0</code> , <code>IOS_12_4</code> or <code>ASA_IOS_7_0_1</code> .

#### ***Attribute.scriptTimeout***

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

#### ***Attribute.useUpdateScriptType***

Specifies whether the default, revised or replacement update script should be used. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### ***Attribute.revisedUpdateScriptFilename***

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

#### ***Attribute.useVerifyScriptType***

Specifies whether the default, revised, or replacement verify script should be used. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### ***Attribute.revisedVerifyScriptFilename***

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

#### ***Attribute.userNameEntryPrompt***

A regular expression that matches the prompt that is produced by the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

#### ***Attribute.passwordEntryPrompt***

A regular expression that matches the prompt that is produced by the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si)(.*password(\\sfor :).*)	valid regular expression syntax

***Attribute.passwordConfirmationPrompt***

A regular expression that matches the remote host prompt that is produced when the host requests a password confirmation.

Required	Default Value	Valid Values
no	AIX: (?si).*?new password.*? All other platforms: (?si).*?password:.*?	valid regular expression syntax

***Attribute.passwordChangePrompt***

A regular expression that matches the prompt produced by the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*?change your password.*?	valid regular expression syntax

***Cisco Target Account CLI Parameters***

To add an Active Directory target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

***Attribute.otherAccount***

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

***Attribute.protocol***

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH, TELNET

***Attribute.pwType***

The credential type; whether it pertains to a user or privileged (or "enable") account.

Required	Default Value	Valid Values
yes	user	user, privileged

**Attribute.useOtherPrivilegedAccount**

Required	Default Value	Valid Values
yes	false	true, false

**Attribute.otherPrivilegedAccount**

Required	Default Value	Valid Values
no	N/A	a valid target account ID

**Attribute.changeAuxLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**Attribute.changeConsoleLoginPassword**

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.changeVtyLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**Attribute.numVTYPorts**

Required	Default Value	Valid Values
yes if changeVtyLoginPassword is true	N/A	1-15

**Cisco CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=www.ca.com
TargetApplication.type=CiscoSSH TargetApplication.name=Cisco
Attribute.extensionType=CiscoSSH Attribute.useDefaultUpdateScript=true
Attribute.useDefaultVerifyScript=true
```

```
cmdName=addTargetAccount TargetServer.hostName=www.ca.com TargetApplication.name=Cisco
TargetAccount.userName=account1
TargetAccount.password=password1 Attribute.protocol=SSH2_PASSWORD_AUTH
Attribute.useOtherAccountToChangePassword=false
pwType=user useOtherPrivilegedAccount=false changeAuxLoginPassword=false
changeConsoleLoginPassword=false
changeVtyLoginPassword=true numVTYPorts=1
```

## Cisco Target Connector External API Configuration

id="bodyContent">

This topic describes the required and supported Attributes used when adding or updating a Cisco Target application and target accounts using the External API.

### Cisco Target Application External API Attributes

To add or update a Cisco Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***sshPort***

The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### ***sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***sshStrictHostKeyCheckingEnabled***

Enables or disables strict host key checking. When enabled, Credential Manager compares the public key that is received from the remote host when making a connection to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Required	Default Value	Valid Values
no	false	true, false

#### ***sshKnownHostKey***

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

#### ***sshKnownHostKeyFingerprint***

Contains the fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is used for display purposes only to allow the user to compare one key with another. The fingerprint that is specified must correspond to the specified public host key.

Required	Default Value	Valid Values
no	N/A	a public key fingerprint



**sshUseDefaultCiphers**

Specifies whether the default ciphers should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**sshServerToClientCiphersList**

Specifies the list of ciphers to accept on the inbound data stream from the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

**sshClientToServerCiphersList**

Specifies the list of ciphers to use on the outbound data stream to the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

**sshDetectCiphersList**

Specifies the list of ciphers to detect when connecting to the remote host. Credential Manager does not attempt to use ciphers that are unavailable even if they are specified to use as inbound and outbound ciphers. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

**sshUseDefaultHashes**

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**sshServerToClientHashesList**

Specifies the list of hashes to accept on the inbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if sshUseDefaultHashes is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

**sshClientToServerHashesList**

Specifies the list of hashes to accept on the outbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if sshUseDefaultHashes is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

**sshUseDefaultKeyExchangeAlgorithms**

Specifies whether to use the default key exchange methods when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**hKeyExchangeAlgorithmsList**

Specifies the list of key exchange methods to use when connecting to the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if sshUseDefaultKeyExchangeAlgorithms is false	diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1	A comma-separated list containing one or more of the following values: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1. Do not use spaces in the list.

**sshUseDefaultCompressionAlgorithms**

Specifies whether the default compression methods should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**sshServerToClientCompressionAlgorithmsList**

Specifies the list of compression methods to accept on the inbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A (do not use compression)	comma-separated list containing one or more of the following values: <code>zlib</code> , <code>zlib@openssh.com</code> . Do not use spaces in the list.

### ***sshClientToServerCompressionAlgorithmsList***

Specifies the list of compression methods to use on the outbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
Yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A (do not use compression)	A comma-separated list containing one or more of the following values: <code>zlib</code> , <code>zlib@openssh.com</code> . Do not use spaces in the list.

### ***sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

### ***sshServerHostKeyAlgorithmsList***

Specifies the list of host key types to accept when Credential Manager connects to the remote host.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultServerHostKeyAlgorithms</code> is false	<code>ssh-rsa,ssh-dss</code>	A comma-separated list containing one or more of the following values: <code>ssh-rsa</code> , <code>ssh-dss</code> . Do not use spaces in the list.

### ***telnetSessionTimeout***

When using the Telnet communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

### ***telnetPort***

The port that is used to connect to the UNIX host using Telnet.

Required	Default Value	Valid Values
no	23	0-65536

### ***ciscoVariant***

Specifies the type of Cisco system that is installed on the target server.

Required	Default Value	Valid Values
no	IOS_12_4	IOS_10_0, IOS_12_4 or ASA_IOS_7_0_1.

### ***scriptTimeout***

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

### ***useUpdateScriptType***

Specifies whether the default, revised or replacement update script should be used. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

### ***revisedUpdateScriptFilename***

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

### ***useVerifyScriptType***

Specifies whether the default, revised, or replacement verify script should be used. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

### ***revisedVerifyScriptFilename***

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

### ***userNameEntryPrompt***

A regular expression that matches the prompt that is produced by the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

***passwordEntryPrompt***

A regular expression that matches the prompt that is produced by the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si)(.*?password(\sfor :).*)	valid regular expression syntax

***passwordConfirmationPrompt***

A regular expression that matches the remote host prompt that is produced when the host requests a password confirmation.

Required	Default Value	Valid Values
no	AIX: (?si).*?new password.*? All other platforms: (?si).*?password:.*?	valid regular expression syntax

***passwordChangePrompt***

A regular expression that matches the prompt produced by the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*?change your password.*?	valid regular expression syntax

**Cisco Target Account External API Attributes**

To add a Cisco target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

***otherAccount***

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

***protocol***

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH, TELNET

***pwType***

The credential type; whether it pertains to a user or privileged (or "enable") account.

Required	Default Value	Valid Values
yes	user	user, privileged

***useOtherPrivilegedAccount***

Required	Default Value	Valid Values
yes	false	true, false

***otherPrivilegedAccount***

Required	Default Value	Valid Values
no	N/A	a valid target account ID

***changeAuxLoginPassword***

Required	Default Value	Valid Values
no	N/A	true, false

***changeConsoleLoginPassword***

Required	Default Value	Valid Values
yes	N/A	true, false

***changeVtyLoginPassword***

Required	Default Value	Valid Values
no	N/A	true, false

***numVTYPorts***

Required	Default Value	Valid Values
yes if changeVtyLoginPassword is true	N/A	1-15

**Cisco Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "CiscoApp",
  "applicationType": "CiscoSSH",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "sshSessionTimeout": "",
    "instance": "",
```

```

    "passwordEntryPrompt": "",
    "sshDetectCiphersList": "",
    "sshClientToServerCiphersList": "",
    "sshClientToServerCompressionAlgorithmsList": "",
    "passwordChangePrompt": "",
    "telnetSessionTimeout": "",
    "useUpdateScriptType": "DEFAULT",
    "sshServerHostKeyAlgorithmsList": "",
    "sshUseDefaultCiphers": "true",
    "userNameEntryPrompt": "",
    "sshUseDefaultHashes": "true",
    "sshKeyExchangeAlgorithmsList": "",
    "telnetPort": "",
    "sslEnabled": "",
    "sshUseDefaultKeyExchangeAlgorithms": "true",
    "passwordConfirmationPrompt": "",
    "sshPort": "",
    "ciscoVariant": "IOS_12_4",
    "sshServerToClientCiphersList": "",
    "useVerifyScriptType": "DEFAULT",
    "sshKnownHostKey": "",
    "sshKnownHostKeyFingerprint": "",
    "sshUseDefaultCompressionAlgorithms": "true",
    "sslPort": "",
    "sshUseDefaultServerHostKeyAlgorithms": "true",
    "scriptTimeout": "",
    "mbean": "",
    "sshClientToServerHashesList": "",
    "port": "",
    "sshServerToClientHashesList": "",
    "sshServerToClientCompressionAlgorithmsList": "",
    "sshStrictHostKeyCheckingEnabled": "false"
  },
  "passwordCompositionPolicyId": null
}

```

### **Cisco Target Account External API Example**

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts

```

{
  "accountName": "CiscoAcc",
  "attributes": {
    "verifyThroughOtherAccount": "",
    "changeConsoleLoginPassword": "false",
    "useOtherPrivilegedAccount": "false",
    "discoveryAllowed": "f",
    "changeAuxLoginPassword": "false",
    "changeVtyLoginPassword": "false",
    "pwType": "user",
    "protocol": "SSH2_PASSWORD_AUTH",
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "f",

```

```

"descriptor1": "",
"useOtherAccountToChangePassword": "false",
"numVTYPorts": "1",
"otherPrivilegedAccount": "-1"
},
"cacheBehavior": "useCacheFirst",
"cacheDuration": "30",
"password": "sample",
"passwordViewPolicyId": 1000,
"privileged": "t",
"synchronize": "f",
"useAliasNameParameter": "f"
}

```

**NOTE**

```

"useOtherAccountToChangePassword": "false" false/true values only
"changeConsoleLoginPassword": "false" false/true values only
"useOtherPrivilegedAccount": "false" false/true values only
"changeAuxLoginPassword": "false", false/true values only
"changeVtyLoginPassword": "false", false/true values only

```

## Add an HP Service Manager Target Connector

The HP Service Manager target connector lets you integrate with HP Service Manager service desk application. For all the steps necessary to configure integration with HP Service Manager, see [HP Service Manager Integration](#).

## Add an IBM i Target Connector

The IBM i (formerly AS/400) target connector manages user accounts and provides password synchronization functionality for iSeries IBM midrange systems.

**NOTE**

Port 8475 must be open on the IBM i device for this connector to function. For SSL/TLS connectivity, port 9475 must be open.

The IBM i connector supports SSL/TLS connections to endpoint systems running OS/400, i5/OS, or IBM i. On the IBM i platform, the targets must be at these PTFs (Program Temporary Fix) maintenance levels:

- V7R3: SI65622
- V7R2: SI65619
- V7R1: SI65613

To add the target connector using the CLI, see the [IBM i Target CLI Configuration](#).

To add the target connector using the external API, see [IBM i Target Connector External API Configuration](#).

### Add an IBM i Target Application and Connector

The IBM i application type defaults to using SSL/TLS. If you upgrade an existing IBM i (or AS/400) application, it does not use SSL/TLS until you enable it. If you are adding a new IBM i application that does not support SSL or TLS, you must disable SSL/TLS.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Applications**.



2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **IBM i**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, the appliance uses the default policy. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. On the **IBM i** tab, confirm that **SSL/TLS Enabled** checkbox is selected. Keeping the box selected to ensure the certificate is a trusted source. Clear the check box to disable SSL/TLS communication.
7. Select **OK**

Any password verification or changes to IBM i target accounts for this application now use an SSL/TLS connection. If your IBM i endpoint does not support SSL/TLS connections, an error occurs.

#### NOTE

Next Step: [Add a target account to the target application.](#)

## IBM i Target CLI Configuration

This topic contains the parameters to add IBM i target applications and target accounts:

### IBM i Target Connector CLI Parameters

To add an IBM i target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### *TargetApplication.type*

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	AS400

#### *Attribute.sslEnabled*

Specify whether to use a secure (SSL or TLS) connection.

Required	Default Value	Valid Values
yes	true	true, false

### IBM i Target Account CLI Parameters

To add an IBM i target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

#### *Attribute.useOtherAccountToChangePassword*

Specify whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.otherAccount**

Specify which other account to use to perform password change requests.

Required	Default Value	Valid Values
If <code>Attribute.useOtherAccountToChangePassword</code> is true, set this parameter to yes	N/A	A valid target account ID

**IBM i CLI Examples**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
```

```
TargetApplication.name=my_AS400_app TargetApplication.type=AS400
```

```
Attribute.extensionType=AS400 Attribute.sslEnabled=true
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
```

```
TargetApplication.name=my_AS400_app TargetAccount.userName=admin
```

```
TargetAccount.password=p@ssw0rd Attribute.extensionType=AS400
```

**IBM i Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating an IBM i (AS400) Target Application using the External API:

**IBM i Target Application External API Attributes**

To add or update an IBM i (aka AS 400) Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***sslEnabled***

Specify whether to use a secure (SSL or TLS) connection.

Required	Default Value	Valid Values
yes	true	true, false

**IBM i Target Account External API Attributes**

To add an IBM i (aka As 400) target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***useOtherAccountToChangePassword***

Specify whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

### ***otherAccount***

Specify which other account to use to perform password change requests.

Required	Default Value	Valid Values
If useOtherAccountToChangePassword is true, set this parameter to yes	N/A	A valid target account ID

### **IBM i Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "AS400",
  "applicationType": "AS400",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "sslEnabled": "false"
  },
  "passwordCompositionPolicyId": null
}
```

### **IBM i Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "AS400Acc",
  "attributes": {
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "discoveryAllowed": "f",
    "useOtherAccountToChangePassword": "false",
    "unlockLockedAccount": "f"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
```

```

    "privileged":"t",
    "synchronize":"f",
    "useAliasNameParameter":"f"
}

```

#### NOTE

"useOtherAccountToChangePassword": "false" false/true values only

## Add a Juniper Junos Target Connector

This target connector provides password synchronization functionality for Juniper Junos® accounts.

To add the target connector using the CLI, see [Juniper Junos Target CLI Configuration](#).

To add the target connector using the external API, see [Juniper Junos Target Connector External API Configuration](#).

### Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Juniper Junos**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions
6. On the Juniper Junos tab, configure the following fields:
  - **Connect Timeout**: enter the timeout for connecting to the directory in milliseconds. Default: 60000
  - **Read Timeout**: enter the timeout for reading from the directory, in milliseconds. Default: 5000.
  - **SSH Port**: Specify the port for secure connections. Default: 22
7. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application](#).

## Juniper Junos Target CLI Configuration

This topic contains the parameters for adding Juno Junos target applications and target accounts:

### Junos Target Connector CLI Parameters

To add a Junos target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	juniper

#### **Attribute.extensionType**

The attribute extension type

Required	Default Value	Valid Values
yes	N/A	juniper

#### **Attribute.sshPort**

The port that is used to connect to the Juniper host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

#### **Attribute.connectTimeout**

Specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	60000	1000-99999

#### **Attribute.readTimeout**

Required	Default Value	Valid Values
no	5000	1000-99999

### **Junos Target Account CLI Parameters**

To add a Junos target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

#### **Attribute.extensionType**

Required	Default Value	Valid Values
yes	N/A	juniper

#### **Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

#### **Attribute.otherAccount**

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
If <code>Attribute.useOtherAccountToChangePassword</code> is true, set to yes	N/A	a valid target account ID.

### **Junos CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=JP1

TargetApplication.type=juniper Attribute.extensionType=juniper Attribute.sshPort=22
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=FW1

TargetAccount.UserName=admin TargetAccount.password=P@ssw0rd
Attribute.extensionType=juniper Attribute.useOtherAccountToChangePassword=false
```

## **Juniper Junos Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating a Juniper Junos Target Application using the External API

This topic describes the required and supported Attributes used when adding or updating a Juniper Junos Target Application using the External API:

### **Junos Target Application External API Attributes**

To add or update a Junos Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

The attribute extension type

Required	Default Value	Valid Values
yes	N/A	juniper

#### **sshPort**

The port that is used to connect to the Juniper host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

#### **connectTimeout**

Specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	60000	1000-99999

#### **readTimeout**

Required	Default Value	Valid Values
no	5000	1000-99999

### **Junos Target Account External API Attributes**

To add a Junos target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **extensionType**

Required	Default Value	Valid Values
yes	N/A	juniper

#### **useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

#### **otherAccount**

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
If useOtherAccountToChangePassword is true, set to yes	N/A	a valid target account ID.

### **Junos Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "JuniperApp",
  "applicationType": "juniper",
  "attributes": {
    "connectTimeout": "60000",
```

```

        "readTimeout":"5000",
        "sshPort":"22"
    }
}

```

### **Junos Target Account External API Example**

```

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
    "accountName":"JuniperAct",
    "attributes":{
        "useOtherAccountToChangePassword":"false",
        "descriptor1":"sample descriptor1"
    },
    "cacheBehavior":"useCacheFirst",
    "cacheDuration":"30",
    "password":"sample",
    "passwordViewPolicyId":1000,
    "privileged":"t",
    "synchronize":"f",
    "useAliasNameParameter":"f"
}

```

## **Add an LDAP Target Connector**

Use the LDAP target connector to manage any accounts that support the OpenLDAP V3 protocol. Optionally, you can configure the LDAP connector for SSL communication.

To add the target connector using the CLI, see the [LDAP Target Connector CLI Configuration](#).

To add the target connector using the external API, see [LDAP Target Connector External API Configuration](#).

### **Add the Target Application and Connector**

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name**: Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name**: Application names must be unique for a given target server.
4. In the **Application Type** field, select **LDAP**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and A maximum length of 16 characters, with no character restrictions.
6. On the **LDAP Details** tab, configure the following fields:
  - **Protocol**: Select either LDAP or LDAPS (SSL).
  - **Server Type**: Specify the LDAP server type:



- **OpenLDAP:** A server running an OpenLDAP implementation
  - **Other:** A server running any other LDAP implementation
  - **CA LDAP for ACF2:** A CA LDAP Server configured with the ACF2 backend security option
  - **CA LDAP for Top Secret:** A CA LDAP Server configured with the Top Secret backend security option
  - **CA LDAP for RACF:** A CA LDAP Server configured with the RACF backend security option
  - **Port:** Enter the port that the LDAP application uses.
  - **Base-64 encoded x.509 Certificate:** If the protocol is SSL, a certificate is required. Search for a certificate.
  - **Connect Timeout:** Enter the time in milliseconds that Credential Manager waits before aborting the attempt to connect to the server. The value defaults to 3000.
  - **Read Timeout:** Enter the time in milliseconds that Credential Manager waits before aborting the request to the server for data. The read timeout applies to the LDAP response from the server, after the initial connection is established with the server.
7. On the **Additional LDAP Attributes for Password Modification** tab, specify the attribute name/value pairs to be updated with password modifications.
- If these attributes are not part of your LDAP schema, an error can occur during password modification. For the OpenLDAP **shadowLastChange** attribute, the appliance provides the dynamic value **%EPOCH\_DAYS%**, which calculates to the current number of days from the epoch (1/1/1970). **%EPOCH\_DAYS%** is the only available dynamic attribute.
- Select on the + (plus) sign on the page and provide the following values:
- **Attribute Name:** The name of the LDAP attribute to pass, such as `shadowLastChange`.
  - **Attribute Value:** The value to send for that LDAP attribute, such as `%EPOCH_DAYS%`.
8. To enable Account Discovery using this account, select the **Account Discovery** tab and enter values in at least the two required fields.
- Base DN (optional)
  - Account Object (required) is an objectClass name corresponding to accounts or users in the directory.
  - Name Attribute (required) denotes an account name.
  - Filter (optional) allows addition of an optional filter string to limit your results.
- For more information, see your LDAP provider documentation.

#### NOTE

Next Step: [Add a target account to the target application.](#)

### Add LDAP Target Account Details

When you select **Add from the Target, Accounts**, the Account Details panel opens. When you select an LDAP Application Name, extra fields appear specific to LDAP accounts.

**DN:** Enter a Distinguished Name for the LDAP Account to use.

**Change Process:** Set to one of these choices:

- Account can change its own password.
- Use the following account to change the password. Search to select an account.

### LDAP Target Connector CLI Configuration

This topic contains the parameters for adding the LDAP target application and target accounts:

#### LDAP Target Application CLI Parameters

To add an LDAP target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

**TargetApplication.type**

The target application connector type.

Required	Default Value	Valid Values
Yes	N/A	ldap

**Attribute.port**

The port that is used to connect to the LDAP Server.

Required	Default Value	Valid Values
Yes	N/A	0-65535. The GUI uses default value 389.

**Attribute.protocol**

The protocol that is used to connect to the LDAP server.

Required	Default Value	Valid Values
Yes	clear	clear, ssl

**Attribute.serverType**

The LDAP server type.

Required	Default Value	Valid Values
No	OpenLDAP	CA ACF2, CA Top Secret, CA RACF, Other, OpenLDAP

**NOTE**

If the specified LDAP server type contains a space (for example, CA Top Secret), the entire Attribute.serverType attribute must be enclosed in quotation marks (") as shown in the following example:

```
capam_command capam=10.10.10.10 userID=admin cmdName=addTargetApplication
TargetServer.hostName=myhostname TargetApplication.name=myLDAP
TargetApplication.type=ldap "Attribute.serverType=CA RACF" Attribute.port=389
Attribute.protocol=clear
```

**Attribute.sslCertificate**

The LDAP SSL certificate.

Required	Default Value	Valid Values
Required if the protocol is SSL.	N/A	X.509 digital certificate in BASE64 encoded format

**Attribute.ldapConnectTimeout**

Time in milliseconds that Credential Manager waits before aborting the attempt to connect to the server.

Required	Default Value	Valid Values
No	3000	1000-99999

**Attribute.IdapReadTimeout**

Time in milliseconds that Credential Manager waits before aborting the request to the server for data. The read timeout applies to the LDAP response from the server, after the initial connection is established with the server.

Required	Default Value	Valid Values
No	3000	1000-99999

**LDAP Target Account CLI Parameters**

To add an LDAP target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

**Attribute.useOtherAccountToChangePassword**

This attribute specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
Yes	N/A	true, false

**Attribute.otherAccount**

This attribute specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

**Attribute.userDN**

The distinguished name of the user on the LDAP server.

Required	Default Value	Valid Values
yes	N/A	String.

**LDAP CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myLDAP TargetApplication.type=ldap Attribute.port=389
Attribute.protocol=clear
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myLDAP TargetAccount.userName=admin
TargetAccount.password=p@ssw0rd TargetAccount.cacheBehavior=useCacheFirst
TargetAccount.cacheDuration=21 Attribute.userDN=admin
Attribute.useOtherAccountToChangePassword=false
```

## LDAP Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating an LDAP target application using the External API.

This topic describes the required and supported Attributes used when adding or updating an LDAP target application using the External API. External API Attributes

### LDAP Target Application External API Attributes

To add or update an LDAP Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **port**

The port that is used to connect to the LDAP Server.

Required	Default Value	Valid Values
Yes	N/A	0-65535. The GUI uses default value 389.

#### **protocol**

The protocol that is used to connect to the LDAP server.

Required	Default Value	Valid Values
Yes	clear	clear, ssl

#### **serverType**

The LDAP server type.

Required	Default Value	Valid Values
No	OpenLDAP	CA ACF2, CA Top Secret, CA RACF, Other, OpenLDAP

#### **NOTE**

If the specified LDAP server type contains a space (for example, CA Top Secret), the entire serverType attribute must be enclosed in quotation marks (") as shown in the following example:

```
capam_command capam=10.10.10.10 userID=admin cmdName=addTargetApplication
TargetServer.hostName=myhostname TargetApplication.name=myLDAP
TargetApplication.type=ldap "serverType=CA RACF" Attribute.port=389
Attribute.protocol=clear
```

#### **sslCertificate**

The LDAP SSL certificate.

Required	Default Value	Valid Values
Required if the protocol is SSL.	N/A	X.509 digital certificate in BASE64 encoded format

#### **ldapConnectTimeout**

Time in milliseconds that Credential Manager waits before aborting the attempt to connect to the server.

Required	Default Value	Valid Values
No	3000	1000-99999

### ***ldapReadTimeout***

Time in milliseconds that Credential Manager waits before aborting the request to the server for data. The read timeout applies to the LDAP response from the server, after the initial connection is established with the server.

Required	Default Value	Valid Values
No	3000	1000-99999

### **LDAP Target Account External API Attributes**

To add an LDAP target account that uses the target connector use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***useOtherAccountToChangePassword***

This attribute specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
Yes	N/A	true, false

#### ***otherAccount***

This attribute specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes <i>useOtherAccountToChangePassword</i> is true.	N/A	A valid target account ID.

#### ***userDN***

The distinguished name of the user on the LDAP server.

Required	Default Value	Valid Values
yes	N/A	String.

### **LDAP Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "ldapApp",
  "applicationType": "ldap",
  "attributes": {
    "port": "389",
    "protocol": "clear",
    "serverType": "OpenLDAP",
    "ldapConnectTimeout": "3000",
```

```

        "ldapReadTimeout":"3000"
    }
}

```

### LDAP Target Account External API Example

```

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
    "accountName":"ldapAct",
    "attributes":{
        "useOtherAccountToChangePassword":"false",
        "userDN":"CN=Administrator,CN=Users,DC=broadcom,DC=test"
    },
    "cacheBehavior":"useCacheFirst",
    "cacheDuration":"30",
    "password":"sample",
    "passwordViewPolicyId":1000,
    "privileged":"t",
    "synchronize":"f",
    "useAliasNameParameter":"f"
}

```

## Add an MSSQL Target Connector

Use the MSSQL connector to manage accounts on Microsoft SQL 2000 and later database servers. The Microsoft connector uses JDBC for communication.

To add the target connector using the CLI, see the [MSSQL Target Connector CLI Configuration](#).

To add the target connector using the external API, see [MSSQL Target Connector External API Configuration](#).

### Add the Target Application and the Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **MSSQL**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum of four characters and a maximum of 16 characters, with no character restrictions
6. On the MSSQL tab, configure the following fields:

- **SSL/TLS Enabled** Select this checkbox to enable a secure connection.
- **Port:** Specify the port for secure connections. Default: 1433. You can connect to a named MSSQL server instance that uses dynamic port binding instead of a specific port number. Enter the appropriate MSSQL instance name and leave the Port field empty.

7. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application.](#)

## MSSQL Target Connector CLI Configuration

This topic contains the parameters for adding MSSQL target applications and target accounts:

### MSSQL Target Application CLI Parameters

To add an MSSQL target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	mssql

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	mssql

#### ***Attribute.sslEnabled***

Required	Default Value	Valid Values
	false	true, false

#### ***Attribute.port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535. The GUI uses default value 1433

#### ***Attribute.instance***

The database instance name.

Required	Default Value	Valid Values
no	N/A. If an instance is not specified, the target connector connects with the default database instance.	String.

## MSSQL Target Account CLI Parameters

To add an MSSQL target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

### ***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

### ***Attribute.otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

## MSSQL CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
```

```
TargetApplication.name=myMSsql TargetApplication.type=mssql
```

```
Attribute.extensionType=mssql Attribute.port=1433
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
```

```
TargetApplication.name=myMSsql TargetAccount.userName=admin
```

```
TargetAccount.password=p@ssw0rd
```

```
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.cacheDuration=21
```

```
Attribute.useOtherAccountToChangePassword=false
```

## MSSQL Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or MSSQL target applications using the External API

This topic describes the required and supported Attributes used when adding or MSSQL target applications using the External API:



**MSSQL Target Application External API Attributes**

To add or update a MSSQL Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***extensionType***

Required	Default Value	Valid Values
yes	N/A	mssql

***sslEnabled***

Required	Default Value	Valid Values
	false	true, false

***port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535. The GUI uses default value 1433

***instance***

The database instance name.

Required	Default Value	Valid Values
no	N/A. If an instance is not specified, the target connector connects with the default database instance.	String.

**MSSQL Target Account External API Attributes**

To add or update a MSSQL Target account using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

**MSSQL Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "mssqlApp",
  "applicationType": "mssql",
  "attributes": { "port": "1433", "sslEnabled": "true" }
}
```

**MSSQL Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts
{
  "accountName": "mssqlAct",
  "attributes": {
    "useOtherAccountToChangePassword": "false",
    "descriptor1": "sample descriptor1"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

**Add an MSSQL Azure Managed Instance Target Connector**

Configure an MSSQL Azure Managed Instance target connector to manage accounts on an Azure SQL Managed Instance.

To add the target connector using the CLI, see the [MSSQL Target Connector CLI Configuration](#).

To add the target connector using the external API, see [MSSQL Azure Managed Instance Target Connector External API Configuration](#).

**NOTE**

The MSSQL Azure Managed Instance target connector currently only supports IPv4 addressing. (The Microsoft Azure SQL Managed Instance does not currently support IPv6 addressing.)

**Add the Target Application and the Connector**

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name**. Select the search icon and pick a target server that is configured for an Azure SQL Managed Instance target server from the dialog that opens.
  - **Device Name**: Accept the default populated value ("Azure SQL managed instance") or enter your own value.
  - **Application Name**: Enter a unique name for the application.
4. In the **Application Type** field, select **MSSQL Azure Managed Instance**.
5. (Optional) Select a password composition policy.

If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum of four characters and a maximum of 16 characters, with no character restrictions

6. On the **MSSQL Azure Managed Instance** tab, configure the following fields:
  - **SSL/TLS Enabled** Select this checkbox to enable a secure connection.
  - **Port:** Specify the port for secure connections. Default: 1433.
7. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application.](#)

## MSSQL Azure Managed Instance Target Connector CLI Configuration

This topic contains the parameters for adding MSSQL Azure Managed Instance target applications and target accounts:

### MSSQL Azure Managed Instance Target Application CLI Parameters

To add an MSSQL Azure Managed Instance target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	mssqlAzureMI

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	mssqlAzureMI

#### ***Attribute.sslEnabled***

Required	Default Value	Valid Values
	false	true, false

#### ***Attribute.port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535. The GUI uses default value 1433

#### ***Attribute.instance***

The database instance name.

Required	Default Value	Valid Values
no	N/A. If an instance is not specified, the target connector connects with the default database instance.	String.

## MSSQL Azure Managed Instance Target Account CLI Parameters

To add an MSSQL Azure Managed Instance target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

### ***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

### ***Attribute.otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

## MSSQL Azure Managed Instance CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=mssqlAzureMIAppTargetApplication.type=mssql
Attribute.extensionType=mssqlAzureMI Attribute.port=1433
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=mssqlAzureMITargetAccount.userName=admin TargetAccount.password=p@ssw0rd
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.cacheDuration=21
Attribute.useOtherAccountToChangePassword=false
```

## MSSQL Azure Managed Instance Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating MSSQL Azure Managed Instance target applications using the External API.

This topic describes the required and supported Attributes used when adding or updating MSSQL Azure Managed Instance target applications using the External API:

### **MSSQL Azure Managed Instance Target Application External API Attributes**

To add or update a MSSQL Azure Managed Instance target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

Required	Default Value	Valid Values
yes	N/A	mssqlAzureMI

***sslEnabled***

Required	Default Value	Valid Values
	false	true, false

***port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535. The GUI uses default value 1433

***instance***

The database instance name.

Required	Default Value	Valid Values
no	N/A. If an instance is not specified, the target connector connects with the default database instance.	String.

**MSSQL Azure Managed Instance Target Account External API Attributes**

To add or update a MSSQL Azure Managed Instance Target account using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

**MSSQL Azure Managed Instance Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "mssqlAzureMIApp",
  "applicationType": "mssqlAzureMI",
  "attributes": {"port": "1433", "sslEnabled": "true"}
}
```

## **MSSQL Azure Managed Instance Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts
{
  "accountName":"mssqlAzureMIAct",
  "attributes":{
    "useOtherAccountToChangePassword":"false",
    "descriptor1":"sample descriptor1"
  },
  "cacheBehavior":"useCacheFirst",
  "cacheDuration":"30",
  "password":"sample",
  "passwordViewPolicyId":1000,
  "privileged":"t",
  "synchronize":"f",
  "useAliasNameParameter":"f"
}
```

## **Add a MySQL Target Connector**

This target connector provides password synchronization<sup>1</sup> functionality for MySQL 5 databases.

### **NOTE**

When a target application is configured for MySQL on a Linux, UNIX, or Solaris server, associated target account credentials may fail to synchronize because of time zone nomenclature incompatibility. For more information, including a workaround, see [Known Issues](#).

To add the target connector using the CLI, see [MySQL Target Connector CLI Configuration](#).

To add the target connector using the external API, see [MySQL Target Connector External API Configuration](#).

## **Add the Target Application and the Connector**

**Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **MYSQL**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. This policy specifies a minimum of four characters and a maximum of 16 characters with no character restrictions
6. On the MYSQL tab, enter a value for the DB Port field, which specifies the port on which the MySQL is listening. The default port is 3306.
7. Select **OK**.

### **NOTE**

Next Step: [Add a target account to the target application](#).

## MySQL Target Connector CLI Configuration

This topic contains the parameters for adding MSSQL target applications and target accounts:

### MySQL Target Application CLI Parameters

To add a MySQL target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	MySQL

#### ***Attribute.port***

The target application port.

Required	Default Value	Valid Values
yes	3306	0-65535

### MySQL Target Account CLI Parameters

To add a MSSQL target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

#### ***Attribute.schema***

The name of the database schema to which the account belongs.

Required	Default Value	Valid Values
yes	N/A	String

#### ***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

#### ***Attribute.otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

#### ***Attribute.hostNameQualifier***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	MySQL wildcard (%)	A valid target account ID.

### MySQL CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=MySQL01
TargetApplication.type=MySQL Attribute.extensionType=MySQL Attribute.port=3306

cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=MySQL01
TargetAccount.userName=admin TargetAccount.password=p@ssw0rd
TargetAccount.cacheAllow=true TargetAccount.cacheDuration=21
Attribute.extensionType=MySQL Attribute.useOtherAccountToChangePassword=false
```

## MySQL Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a MSSQL Target Application using the External API:

### MySQL Target Application External API Attributes

To add or update a MySQL application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **port**

The target application port.

Required	Default Value	Valid Values
yes	3306	0-65535

### MySQL Target Account External API Attributes

To add a MySQL target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **schema**

The name of the database schema to which the account belongs.

Required	Default Value	Valid Values
yes	N/A	String

#### **useOtherAccountToChangePassword**



Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

### ***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if useOtherAccountToChangePassword is true.	N/A	A valid target account ID.

### ***hostNameQualifier***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if useOtherAccountToChangePassword is true.	MySQL wildcard (%)	A valid target account ID.

### **MySQL Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "mysqlApp",
  "applicationType": "mysql",
  "attributes": { "port": "3306" }
}
```

### **MySQL Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "mysqlAct",
  "attributes": {
    "useOtherAccountToChangePassword": "false",
    "schema": "master"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
```

}

## Add an Oracle Target Connector

Use the Oracle target connector to manage accounts for an Oracle database and Oracle Internet Directory (OID). The configuration procedure for Oracle Internet Directory is the same as for an Oracle database. The Oracle connector uses JDBC to communicate.

To add the target connector using the CLI, see [Oracle Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Oracle Target Connector External API Configuration](#).

### Add the Target Application and Connector

Follow these steps in the UI:

1. Select Credentials, Manage Targets, Applications.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Oracle**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. On the Oracle tab, specify values for the following settings:
  - **SSL/TLS Enabled:** Select this box to establish a secure connection using SSL or TLS. Selecting SSL\TLS and specifying a Distinguished Name (DN) value enforces DN Matching.
  - **DB Port (Required):** Specify the port that the database listens on. Default: 1521
  - **OID (LDAP) Port:** If you are connecting to an Oracle Internet Directory service, specify the port that the service is listening on. Default: 3060
  - **Base 64-encoded x.509 certificate:** This certificate includes a public key, digital signature, and information about both the identity associated with the certificate and its issuing certificate authority (CA). This certificate is used to verify the identity of the entity presenting it.
  - **SSL Certificate Server DN:** The Distinguished Name used to force the server's DN to match its service name. Providing a value means SSL ensures that the certificate is from the server. **Note:** This field is only applicable if the SSL/TLS option is enabled.
7. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application](#).

## Oracle Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding Oracle target applications and target accounts.

### Oracle Target Application CLI Parameters

To add an Oracle target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

**Attribute.sslCertServerDN**

The Distinguished Name (DN) of the Oracle Server.

Required	Default Value	Valid Value
no	None	string

**TargetApplication.type**

The target application connector type.

Required	Default Value	Valid Value
yes	None	oracle

**Attribute.extensionType**

The target application extension type.

Required	Default Value	Valid Value
yes	None	oracle

**Attribute.port**

The port that is used to connect to an Oracle Database server.

Required	Default Value	Valid Value
yes	None	0-65535

**Attribute.oidport (Oracle Internet Directory)**

The port that is used to connect to an Oracle Internet Directory (LDAP) server. Do not specify for Oracle Database.

Required	Default Value	Valid Value
yes	None	0-65535

**Attribute.sslEnabled**

Specifies whether SSL is enabled.

Required	Default Value	Valid Values
yes	None	true, false

**Attribute.sslCertificate**

The SSL certificate.

Required	Default Value	Valid Value
Required if the protocol is SSL	None	X.509 digital certificate in BASE64 encoded format

**Oracle Target Account CLI Parameters**

To add an Oracle target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

***Attribute.schema (Oracle Database)***

The name of the database schema to which the account belongs. Do not specify this option for Oracle Internet Directory.

Required	Default Value	Valid Value
yes (for Oracle database)	None	string

***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	None	true, false

***Attribute.otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Value
yes, if Attribute.useOtherAccountToChangePassword is true	None	A valid target account ID

***Attribute.useOid (Oracle Database)***

Specifies the connection type in use. Do not specify this option for Oracle Internet Directory.

Required	Default Value	Valid Values
yes	false	true, false

***Attribute.sid (Oracle Internet Directory)***

Specifies the System Identifier (SID) of the Oracle Internet Directory database instance. Do not specify this option for Oracle Database.

Required	Default Value	Valid Value
yes (for Oracle Internet Directory)	None	A valid SID (as specified during Oracle database installation). Example: orcl

***Attribute.cn (Oracle Internet Directory)***

Specifies the Common Name (CN) for an Oracle Context. Do not specify this option for Oracle Database.

Required	Default Value	Valid Value
yes	cn=OracleContext	A valid CN

***Attribute.racService***

Specifies whether the schema is a RAC service name.

Required	Default Value	Valid Values
yes	None	true, false

#### ***Attribute.sysdbaAccount***

Specifies whether this user must authenticate as the `Sysdba` role.

Required	Default Value	Valid Values
yes	None	true, false

#### ***Attribute.replaceSyntax***

Specifies whether the `REPLACE` syntax must be used for changing the password that is associated with `otheraccounts`.

Required	Default Value	Valid Values
yes	None	true, false

### **Examples for Oracle Database**

To specify an Oracle target application:

```
cmdName=addTargetApplication TargetServer.hostName=rh72
  TargetApplication.name=myOracle
TargetApplication.type=oracle Attribute.port=1521
```

```
cmdName=addTargetAccount TargetServer.hostName=rh72
  TargetApplication.name=myOracle TargetAccount.userName=system
TargetAccount.password=myPasswd Attribute.schema=XE
  Attribute.useOtherAccountToChangePassword=false
TargetAccount.privileged=true
  TargetAccount.synchronize=true Attribute.useOid=false
```

To specify a synchronized Oracle target account:

```
cmdName=addTargetAccount TargetServer.hostName=rh72
  TargetApplication.name=myOracle
TargetAccount.userName=system TargetAccount.password=myPasswd
  Attribute.schema=XE
```

```
Attribute.useOtherAccountToChangePassword=false TargetAccount.privileged=true
```

```
TargetAccount.synchronize=true Attribute.useOid=false
```

### **Examples for Oracle Internet Directory**

To specify an Oracle Internet Directory target application:

```
cmdName=addTargetApplication TargetServer.hostName=rh72.forwardinc.com
  TargetApplication.name=myOracle
TargetApplication.type=oracle Attribute.port=1433 Attribute.oidPort=3060
```

To specify a synchronized Oracle Internet Directory target account:

```
cmdName=addTargetAccount TargetServer.hostName=rh72.forwardinc.com
TargetApplication.name=myOracle
TargetAccount.userName=admin TargetAccount.password=p@ssw0rd
TargetAccount.cacheBehavior=useCacheFirst
TargetAccount.cacheDuration=21 Attribute.sid=orclAttribute.cn=OracleContext Attribute.useOther
Attribute.racService=false Attribute.sysdbaAccount=false
Attribute.replaceSyntax=false
```

## Oracle Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating an Oracle Target Application using the External API.

### Oracle Target Application External API Attributes

To add or update an Oracle Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***sslCertServerDN***

The Distinguished Name (DN) of the Oracle Server.

Required	Default Value	Valid Value
no	None	string

#### ***extensionType***

The target application extension type.

Required	Default Value	Valid Value
yes	None	oracle

#### ***port***

The port that is used to connect to an Oracle Database server.

Required	Default Value	Valid Value
yes	None	0-65535

#### ***oidport (Oracle Internet Directory)***

The port that is used to connect to an Oracle Internet Directory (LDAP) server. Do not specify for Oracle Database.

Required	Default Value	Valid Value
yes	None	0-65535

#### ***sslEnabled***

Specifies whether SSL is enabled.

Required	Default Value	Valid Values
yes	None	true, false

### ***sslCertificate***

The SSL certificate.

Required	Default Value	Valid Value
Required if the protocol is SSL	None	X.509 digital certificate in BASE64 encoded format

### **Oracle Target Account External API Attributes**

To add a xxx target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***schema (Oracle Database)***

The name of the database schema to which the account belongs. Do not specify this option for Oracle Internet Directory.

Required	Default Value	Valid Value
yes (for Oracle database)	None	string

#### ***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	None	true, false

#### ***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Value
yes, if useOtherAccountToChangePassword is true	None	A valid target account ID

#### ***useOid (Oracle Database)***

Specifies the connection type in use. Do not specify this option for Oracle Internet Directory.

Required	Default Value	Valid Values
yes	false	true, false

#### ***sid (Oracle Internet Directory)***

Specifies the System Identifier (SID) of the Oracle Internet Directory database instance. Do not specify this option for Oracle Database.

Required	Default Value	Valid Value
yes (for Oracle Internet Directory)	None	A valid SID (as specified during Oracle database installation). Example: orcl

### ***cn (Oracle Internet Directory)***

Specifies the Common Name (CN) for an Oracle Context. Do not specify this option for Oracle Database.

Required	Default Value	Valid Value
yes	cn=OracleContext	A valid CN

### ***racService***

Specifies whether the schema is a RAC service name.

Required	Default Value	Valid Values
yes	None	true, false

### ***sysdbaAccount***

Specifies whether this user must authenticate as the Sysdba role.

Required	Default Value	Valid Values
yes	None	true, false

### ***replaceSyntax***

Specifies whether the REPLACE syntax must be used for changing the password that is associated with otheraccounts .

Required	Default Value	Valid Values
yes	None	true, false

### **Oracle Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "OracleApp",
  "applicationType": "oracle",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "sslCertificate": "-----BEGIN CERTIFICATE-----atNlKIQ9DYYVvJMkmUgaq5HiALrRH/
qZut58K64vOgl7r5O0SS5jT1RwwKDq -----END CERTIFICATE-----",
    "port": "2484",
    "extensionType": "oracle",
    "sslEnabled": "true",
```



```

    "oidPort": "3060"
  },
  "passwordCompositionPolicyId": null
}

```

### **Oracle Target Account External API Example**

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts

```

{
  "accountName": "oracleAcc",
  "attributes": {
    "schema": "schema1",
    "discoveryAllowed": "f",
    "sysdbaAccount": "false",
    "useOid": "false",
    "cn": "",
    "sid": "",
    "racService": "false",
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "false",
    "descriptor1": "",
    "replaceSyntax": "false",
    "useOtherAccountToChangePassword": "false"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}

```

## **Add a Palo Alto Target Connector**

Use the Palo Alto connector to manage accounts on Palo Alto routers that use PAN-OS software. This connector uses the SSHv2 protocol for communication.

To add the target connector using the CLI, see [Palo Alto Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Palo Alto Target Connector External API Configuration](#).

### **Add the Target Application and Connector**

**Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.

2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name**. Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name**. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Palo Alto**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select the **SSH-2** tab and enter values for the following two fields to configure the connection.
  - Port: Enter the port that connects to the Palo Alto host using SSH. Default: 22
  - Communication Timeout: Specify the amount of time the appliance waits for communication from the remote target server before ending the connection. Default: 60000 milliseconds
7. Select **OK**.

### **Use a Script to Simplify Communication (Optional)**

The Palo Alto target connector includes a large amount of low-level code to handle communications with the remote host. Credential Manager can use a script processor to simplify such communications.

The script processor (written in Java) executes a high-level version of the logic for manipulating credentials on remote hosts. Two scripts allow different levels of testing and production use. One script verifies passwords while the other script updates passwords.

A set of default scripts is provided with the appliance. To use the default scripts, configure a set of default prompts and command values.

When adding target applications and target accounts, you can configure the script settings with the UI or the CLI.

### ***Generate the Script***

**Follow these steps to generate the script in the UI:**

1. Select the **Script Processor** tab.
2. In the Script Timeout field, enter the amount of time, from 5000 through 59999 milliseconds, that the appliance waits to receive expected input from the remote host. Default: 5000
3. When specified, the following prompts and commands are substituted into appropriate locations (variables) in the default scripts. You can enter a substitute string.
  - **Password Change Prompt**: A regular expression that matches the remote host prompt when it requests that a password be changed because it has expired.  
Default: (?si).\*?change your password.\*?
  - **Password Confirmation Prompt**: A regular expression that matches the remote host prompt when it requests a password confirmation.  
Default: (?si).\*?password:.\*?
  - **Password Entry Prompt**: A regular expression that matches the remote host prompt when it requests a password.  
Default: (?si) (. .\*?password(\sfor|:). .\*?)
  - **User Name Entry Prompt**: A regular expression that matches the remote host prompt when it requests a user name.  
Default: (?si).\*?login:.\*?

### ***Apply the Script to Update and Verify Credentials***

**Follow these steps:**

1. Select the **Credentials Script** tab.

2. In the Update and Verify sections, select one of the available options:

**TIP**

We recommend that you use the default script. If a revised script is required, contact CA Services.

- **Use the default script**  
Select this option for the appliance to use the default script that is provided with the release. If changes to the script logic are required, contact CA Services.
- **Use a revised default script (requires patch)**  
Select this option to use a revised script that is provided by CA Services. Select the appropriate script from the drop-down list.
- **Use a replacement script**  
Select this option to use a replacement script. When selected, this option opens the **Replacement Script** text box. Paste the new script in the box, and try the operation.  
You might have to try more than one replacement script so the appliance conforms to your OS environment. Only edit the replacement scripts with assistance from CA Services.

**WARNING**

**Customer Responsibilities for Custom Scripts:** If you build custom scripts, you are responsible for the operation between the target application and the target endpoint. CA Technologies is responsible for operation up to the point where PAM passes information to the custom target application. After that point, you are responsible for how the custom script handles communication at an operational and security level.

**NOTE**

Next Step: [Add a target account to the target application.](#)

## Palo Alto Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding Active Directory target applications and target accounts.

### Palo Alto Add Target Application CLI Parameters

To add a Palo Alto target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### TargetApplication.type

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	Palo Alto

#### Attribute.sshPort

Indicates the port that is used to connect to the host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### Attribute.sshSessionTimeout

When using an SSH connection, specifies the amount of time in milliseconds that Credential Manager waits for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### **Attribute.scriptTimeout**

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

#### **Attribute.useUpdateScriptType**

Specifies whether the default, revised, or replacement update script should be used. If you require a revised or replacement script, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### **Attribute.revisedUpdateScriptFilename**

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if you require a revised or replacement script.

Required	Default Value	Valid Values
no	N/A	a file name

#### **Attribute.useVerifyScriptType**

Verifies whether the default, revised, or replacement script gets used. If you require a revised or replacement script, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### **Attribute.revisedVerifyScriptFilename**

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if you require a revised or replacement script.

Required	Default Value	Valid Values
no	N/A	a file name

#### **Attribute.userNameEntryPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

**Attribute.passwordEntryPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si)(.*?password(\sfor :).*)?	valid regular expression syntax

**Attribute.passwordConfirmationPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a password be confirmed.

Required	Default Value	Valid Values
no	AIX: (?si).*?new password.*? All other platforms: (?si).*?password:.*?	valid regular expression syntax

**Attribute.passwordChangePrompt**

A regular expression that matches the prompt produced by the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*?change your password.*?	valid regular expression syntax

**Palo Alto Add Target Account CLI Parameters**

To add an Active Directory target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

**Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

**Attribute.otherAccount**

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

**Attribute.protocol**

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH

**Attribute.pwType**

The credential type; whether it pertains to a user or privileged (or "enable") account.

Required	Default Value	Valid Values
yes	user	user, privileged

**Attribute.useOtherPrivilegedAccount**

Required	Default Value	Valid Values
yes	false	true, false

**Attribute.otherPrivilegedAccount**

Required	Default Value	Valid Values
no	N/A	a valid target account ID

**Attribute.changeAuxLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**Attribute.changeConsoleLoginPassword**

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.changeVtyLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**Attribute.numVTYPorts**

Required	Default Value	Valid Values
yes if changeVtyLoginPassword is true	N/A	1-15

**Palo Alto CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=www.ca.com
TargetApplication.type=????? TargetApplication.name=PaloAlto

Attribute.extensionType=????? Attribute.useDefaultUpdateScript=true
Attribute.useDefaultVerifyScript=true
```

```

cmdName=addTargetAccount TargetServer.hostName=www.ca.com
TargetApplication.name=PaloAlto TargetAccount.userName=account1

TargetAccount.password=password1 Attribute.protocol=SSH2_PASSWORD_AUTH
Attribute.useOtherAccountToChangePassword=false

pwType=user useOtherPrivilegedAccount=false changeAuxLoginPassword=false
changeConsoleLoginPassword=false

changeVtyLoginPassword=true numVTYPorts=1

```

## Palo Alto Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a Palo Alto Target Application using the External API.

### **Palo Alto Add Target Application External API Attributes**

To add or update a Palo Alto Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **sshPort**

Indicates the port that is used to connect to the host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### **sshSessionTimeout**

When using an SSH connection, specifies the amount of time in milliseconds that Credential Manager waits for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### **scriptTimeout**

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

#### **useUpdateScriptType**

Specifies whether the default, revised, or replacement update script should be used. If you require a revised or replacement script, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### **revisedUpdateScriptFilename**

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if you require a revised or replacement script.

Required	Default Value	Valid Values
no	N/A	a file name

#### **useVerifyScriptType**

Verifies whether the default, revised, or replacement script gets used. If you require a revised or replacement script, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### **revisedVerifyScriptFilename**

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if you require a revised or replacement script.

Required	Default Value	Valid Values
no	N/A	a file name

#### **userNameEntryPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

#### **passwordEntryPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si)(.*password(\sfor :).*)	valid regular expression syntax

#### **passwordConfirmationPrompt**

A regular expression that matches the prompt produced by the remote host when it requests a password be confirmed.

Required	Default Value	Valid Values
no	AIX: (?si).*?new password.*? All other platforms: (?si).*?password:.*?	valid regular expression syntax



**passwordChangePrompt**

A regular expression that matches the prompt produced by the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*?change your password.*?	valid regular expression syntax

**Palo Alto Add Target Account External API Attributes**

To add a Palo Alto target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

**useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

**otherAccount**

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

**protocol**

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH

**pwType**

The credential type; whether it pertains to a user or privileged (or "enable") account.

Required	Default Value	Valid Values
yes	user	user, privileged

**useOtherPrivilegedAccount**

Required	Default Value	Valid Values
yes	false	true, false

**otherPrivilegedAccount**

Required	Default Value	Valid Values
no	N/A	a valid target account ID

**changeAuxLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**changeConsoleLoginPassword**

Required	Default Value	Valid Values
yes	N/A	true, false

**changeVtyLoginPassword**

Required	Default Value	Valid Values
no	N/A	true, false

**numVTYPorts**

Required	Default Value	Valid Values
yes if changeVtyLoginPassword is true	N/A	1-15

**Palo Alto Target Application External API Example**

POST /api.php/v1/devices.json/{deviceId}/targetApplications

```
{
  "applicationName": "PaloAltoApp",
  "applicationType": "PaloAlto",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "sshPort": "",
    "sshSessionTimeout": "",
    "instance": "",
    "passwordEntryPrompt": "",
    "useVerifyScriptType": "DEFAULT",
    "passwordChangePrompt": "",
    "useUpdateScriptType": "DEFAULT",
    "sslPort": "",
    "userNameEntryPrompt": "",
    "scriptTimeout": "",
    "mbean": "",
    "port": "",
    "extensionType": "PaloAlto",
  }
}
```

```

    "sslEnabled": "",
    "passwordConfirmationPrompt": ""
  },
  "passwordCompositionPolicyId": null
}

```

### **Palo Alto Target Account External API Example**

PaloAlto Target Account external API example

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts

```

{
  "accountName": "PaloAltoAcc",
  "attributes": {
    "pwType": "privileged",
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "discoveryAllowed": "f",
    "useOtherAccountToChangePassword": "f"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}

```

## **Add a RADIUS/TACACS+ Secret Target Connector**

Set up this connector to authenticate users against a RADIUS or TACACS+ server. For configuration instructions, see [Configure RADIUS or TACACS+ for Authentication](#).

## **Add a ServiceNow Target Connector**

The ServiceNow target connector helps you communicate with ServiceNow service management software. For all the configuration steps necessary to integrate with ServiceNow, see [ServiceNow Integration](#).

## **Office365 Integration Messages, SAML IdP and SP Messages**

PAM-CMN-0686 = Default default contact user {0} does not exist.

PAM-CMN-0687 = Invalid default contact method {0} specified.

PAM-CMN-0688 = Device monitor protocol required.

PAM-CMN-0689 = Device monitor port required for protocol {0}.

PAM-CMN-0690 = Device monitor contact required for protocol {0}.

PAM-CMN-0691 = Device monitor contact method required for protocol {0}.

PAM-CMN-0692 = Invalid device monitor protocol specified.

PAM-CMN-0693 = Invalid device monitor port {0} specified for protocol {1}.

PAM-CMN-0694 = Invalid device contact method specified for protocol {0}.

PAM-CMN-0695 = Device monitor contact {0} does not exist.

PAM-CMN-0696 = Maximum buffer size is 8192.

PAM-CMN-0697 = Invalid web session recording quality specified. Valid values are high and low.

PAM-CMN-0698 = Unauthorized attempt to delete policies associated with the Office365 service.

PAM-CMN-0699 = Calculating the certificate fingerprint for IdP {0} failed. The IdP configuration will not be saved.

PAM-CMN-0700 = The SAML SP's {0} is a required field. Please enter a valid value.

PAM-CMN-0701 = The SAML SP's Fully Qualified Hostname is not a valid hostname.

PAM-CMN-0702 = The {0} of Identity Provider {1} is a required field. Please enter a valid value.

PAM-CMN-0703 = Invalid Identity Provider SSO binding specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0704 = The Single Sign On Service URL for Identity Provider {0} is not a valid HTTP URL.

PAM-CMN-0705 = The specified {0} of Identity Provider {1} is invalid. Valid values are: true or false.

PAM-CMN-0706 = The specified certificate for Identity Provider {0} is not a valid PEM certificate.

PAM-CMN-0707 = Invalid Signature Algorithm specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0708 = Invalid Name ID Formats specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0709 = Invalid Authentication Contexts specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0710 = Identity Provider entity IDs must be unique. There are multiple identity providers with the following entity ID(s): {0}.

PAM-CMN-0711 = Invalid SAML version specified for Identity Provider {0}. Valid values are: 1.1, 2.0

PAM-CMN-0712 = CA PAM as SAML SP configuration updated.

PAM-CMN-0713 = Identity Provider friendly names must be unique. There are multiple identity providers with the following friendly name(s): {0}.

PAM-CMN-0714 = Invalid vulnerability reporting level specified. Valid values are 'Log' or 'Log And Warn'.

PAM-CMN-0715 = Invalid vulnerability enabled specified.

PAM-CMN-0716 = The following required fields in the SAML SP configuration must be specified before the configuration can be saved or an IdP can be configured: Entity ID, Fully Qualified Hostname, Certificate Key Pair.

PAM-CMN-0717 = The required field, 'Fully Qualified Hostname', in the SAML configuration on cluster member {0} has not been defined. Please specify a value for the field before downloading metadata.

PAM-CMN-0718 = SAML SP metadata for remote IdP {0} downloaded.

PAM-CMN-0719 = An attempt was made to access the SAML IdP Proxy service when CA PAM is not deployed in a cluster.

PAM-CMN-0720 = An error occurred while completing this request. Please contact your administrator for further assistance.

PAM-CMN-0721 = An attempt was made to access the SAML IdP Proxy service on this node but this node is not the cluster master.

PAM-CMN-0722 = The following remote IdP(s) have been deleted: {0}.

PAM-CMN-0723 = The following remote IdP(s) have been added: {0}.

PAM-CMN-0724 = The id of identity provider {0} is not a valid id: {1}.

PAM-CMN-0725 = Invalid value specified ({0}). Integer expected.

PAM-CMN-0726 = Invalid value specified for SAML Accept RSA-SHA1 Signed Responses. Valid values are: t,f.

PAM-CMN-0727 = Invalid value specified for Client Distribution Intranet URL. Only domain names and IP addresses are allowed.

PAM-CMN-0728 = Invalid port specified for Client Distribution Intranet URL.

PAM-CMN-1818 = No user name supplied for Office 365.

PAM-CMN-1921 = Updated Microsoft Office 365 configuration

PAM-CMN-1922 = Cleared Microsoft Office 365 configuration

PAM-CMN-1923 = Office 365 configuration test: Connected successfully to the supplied URLs

PAM-CMN-1924 = Office 365 configuration test: Error connecting to the supplied URLs

PAM-CMN-2346 = Updated Microsoft Office 365 configuration  
 PAM-CMN-2347 = Cleared Microsoft Office 365 configuration  
 PAM-CMN-2348 = Office 365 configuration test: Connected successfully to the supplied URLs  
 PAM-CMN-2349 = Office 365 configuration test: Error connecting to the supplied URLs

## Add an SPML Target Connector

Use the Service Provisioning Markup Language (SPML) connector to manage any SPML v2.0-compliant providers.

To add the target connector using the CLI, see [SPML Target Connector CLI Configuration](#).

To add the target connector using the external API, see [SPML Target Connector External API Configuration](#).

### Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select SPML v2.0.
5. (Optional) Select a password composition policy.  
 If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. On the SPML v2.0 tab, complete the following fields:
  - Port (optional): The port that is used to connect to the SPML server. Default: 8080
  - Path: Specify the URL to the service. Credential Manager uses this path to communicate to the SPML application.
  - Protocol: Select whether the communication channel is SSL or not.
  - Base-64 encoded X.509 Certificate: Select the certificate for the SSL connection.

#### **NOTE**

Next Step: [Add a target account to the target application](#).

## SPML Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding Active Directory target applications and target accounts.

### SPML Target Connector CLI Parameters

To add an SPML target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	SPML2

**Attribute.extensionType**

Required	Default Value	Valid Values
yes	N/A	SPML2

**Attribute.port**

The port that is used to connect to the SPML server.

Required	Default Value	Valid Values
yes	N/A	0-65535

**Attribute.path**

Path to the SPML service.

Required	Default Value	Valid Values
no	N/A	Text string

**Attribute.protocol**

The protocol that is used to connect to the SPML server.

Required	Default Value	Valid Values
no	clear	clear, ssl

**Attribute.sslCertificate**

The Active Directory SSL certificate.

Required	Default Value	Valid Values
Require if the protocol is SSL .	N/A	X.509 digital certificate in BASE64 encoded format

**SPML Target Account CLI Parameters**

To add an Active Directory target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

**Attribute.extensionType**

Required	Default Value	Valid Values
yes	N/A	SPML2

**Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.otherAccount**

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

### **SPML CLI Example**

```
cmdName=addTargetApplication
TargetServer.hostName=myHostName.myDomain.com TargetApplication.name=spmlAppl
TargetApplication.type=SPML2 Attribute.path=myServletPath Attribute.port=389
cmdName=addTargetAccount
TargetServer.hostName=myhostname.mydomain.com TargetApplication.name=spmlAppl
TargetAccount.userName=admin TargetAccount.password='p@ssw0rd'
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.cacheDuration=21
Attribute.useOtherAccountToChangePassword=false
```

## **SPML Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating a SPML Target Application using the External API.

### **SPML Target Application External API Attributes**

To add or update a SPML Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

Required	Default Value	Valid Values
yes	N/A	SPML2

#### ***port***

The port that is used to connect to the SPML server.

Required	Default Value	Valid Values
yes	N/A	0-65535

#### ***path***

Path to the SPML service.

Required	Default Value	Valid Values
no	N/A	Text string

#### ***protocol***

The protocol that is used to connect to the SPML server.

Required	Default Value	Valid Values
no	clear	clear, ssl

### ***sslCertificate***

The Active Directory SSL certificate.

Required	Default Value	Valid Values
Require if the protocol is SSL .	N/A	X.509 digital certificate in BASE64 encoded format

### **SPML Target Account External API Attributes**

To add a SPML target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

Required	Default Value	Valid Values
yes	N/A	SPML2

#### ***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

#### ***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if useOtherAccountToChangePassword is true.	N/A	A valid target account ID.

### **SPML Target Application External API Example**

SPML2 Target Application external API example

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "SPML2App",
  "applicationType": "SPML2",
  "attributes": {
    "port": "8080",
    "protocol": "clear"
  }
}
```



### **SPML Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "SPML2Act",
  "attributes": {
    "useOtherAccountToChangePassword": "false",
    "databaseName": "master"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

## **Add a Sybase Target Connector**

The Sybase target connector provides password synchronization functionality for Sybase databases.

To add the target connector using the CLI, see [Sybase Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Sybase Target Connector External API Configuration](#).

### **Add the Target Application and the Connector**

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name**. Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name**. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Sybase**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. This policy specifies a minimum of four characters and a maximum of 16 characters with no character restrictions
6. On the **Sybase** tab that appears, specify the following properties:
  - **TLS Enabled**: Specifies whether to enable TLS connections.
  - **DB Port**: Specifies the port on which the database is listening.
  - **Base-64 encoded x.509 Certificate**: If TLS is enabled, the root certificate for the SAP ASE server
7. Select **OK**.

8. (Optional) To configure the Sybase target connector to connect to Sybase servers that are configured to accept only encrypted password authentication, see the next section, [Upload A Sybase Sdk JAR File for the Sybase Target Connector](#).

#### NOTE

Next step (now, or after optionally configuring the Sybase target connector to connect to Sybase servers that are configured to accept only encrypted password authentication): [Add Target Accounts to Target Applications](#).

## Upload a Sybase SDK JAR File for the Sybase Target Connector

The Sybase target connector provides password synchronization functionality for Sybase databases. This content describes how to upload the Sybase SDK JAR file that is required for the Sybase target connector to work.

#### Follow these steps:

1. Obtain a Sybase SDK JAR file from Sybase. We currently support the 16.0 SP02 and SP03 versions of the Sybase JAR:

- SHA256 HASH for 16.0 SP02  
F8EEB645E573F90AECBE63AD7E03642A6DE4A0CE79DE07CEDA9A7DE61EBCDF3B
- SHA256 HASH for 16.0 SP03  
A14856895D44DCFBF15756263EE672F7A4A36A1476F6E43401B995E2DEF86F33

To find the JAR version, run the following command:

```
java -JAR .\jconn4.jar
```

Example output:

```
jConnect (TM) for JDBC(TM)/16.0 SP02 PL08 (Build 27392)/P/EBF28559/JDK 1.6.0/jdbcmain/
OPT/Thu Nov 22 17:40:56 PST 2018
```

2. Copy the following SDK JAR file to a location accessible to the PAM Appliance:  
jconn4.jar
3. Log in to the PAM UI.
4. Select **Configuration, 3rd Party, Sybase**.
5. On the **Upload File** tab, select **Choose File** button and browse for the JAR files individually.
6. Select **Upload** to upload the file.

#### NOTE

If you are load balancing, you have to upload the JAR file to each server. The files are the same for Windows and Linux. There can be only one version of the JAR file at any given time. Uploading different versions of supported JAR files will replace the existing one on the PAM server.

7. On the **Sybase Files** tab, select **Restart PAM** to restart PAM. Wait until the process completes.

#### NOTE

Next Step: [Add the Sybase target application and connector](#).

## Add the Sybase Target Application and Connector

The Sybase target connector provides password synchronization functionality for Sybase databases.

To add the target connector using the CLI, see [Sybase Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Sybase Target Connector External API Configuration](#).

#### Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:

- **Host Name.** Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name.** Application names must be unique for a given target server.
4. In the **Application Type** field, select **Sybase**.
  5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. This policy specifies a minimum of four characters and a maximum of 16 characters with no character restrictions
  6. On the **Sybase** tab that appears, specify the following properties:
    - **TLS Enabled:** Specifies whether to enable TLS connections.
    - **DB Port:** Specifies the port on which the database is listening.
    - **Base-64 encoded x.509 Certificate:** If TLS is enabled, the root certificate for the SAP ASE server
  7. Select **OK**.

**NOTE**

Next Step: [Add a target account to the target application.](#)

## Sybase Target Connector CLI Configuration

This topic contains the parameters for adding Sybase target applications and target accounts:

### Sybase Target Application CLI Parameters

To add a Sybase target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	sybase

#### ***Attribute.sslEnabled***

Required	Default Value	Valid Values
	false	true, false

#### ***Attribute.sslCertificate***

The LDAP SSL certificate.

Required	Default Value	Valid Values
Required if the protocol is SSL.	N/A	X.509 digital certificate in BASE64 encoded format

#### ***Attribute.port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535.

## Sybase Target Account CLI Parameters

To add a Sybase target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

### ***Attribute.schema***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

### ***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	None	true, false

### ***Attribute.otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	sybase

## Sybase CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=rh72 TargetApplication.name=mySybase
TargetApplication.type=sybase Attribute.port=5000
```

```
cmdName=addTargetAccount TargetServer.hostName=rh72 TargetApplication.name=mySybase
TargetAccount.userName=sybaseUser TargetAccount.password=myPasswd
TargetAccount.privileged=true TargetAccount.synchronize=true
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.cacheDuration=30
Attribute.extensionType=sybase Attribute.schema=master
Attribute.useOtherAccountToChangePassword=false
```

## Sybase Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a Sybase Target Application using the External API:

### Sybase Target Application External API Attributes

To add or update a Sybase Target Connector using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***sslEnabled***

Required	Default Value	Valid Values
	false	true, false

#### ***sslCertificate***

The LDAP SSL certificate.

Required	Default Value	Valid Values
Required if the protocol is SSL.	N/A	X.509 digital certificate in BASE64 encoded format

#### ***port***

The target application port.

Required	Default Value	Valid Values
no	N/A	0-65535.

### Sybase Target Account External API Attributes

To add a Sybase target account that uses the target connector use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***schema***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

#### ***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	None	true, false

#### ***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes if useOtherAccountToChangePassword is true.	N/A	A valid target account ID.

### ***extensionType***

Required	Default Value	Valid Values
yes	N/A	sybase

### **Sybase Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "SybaseApp",
  "applicationType": "sybase",
  "attributes": { "port": "5000", "sslEnabled": "false" },
  "description1": "sample description1",
  "description2": "sample description2",
  "passwordCompositionPolicyId": null
}
```

### **Sybase Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "SybaseAct",
  "attributes": {
    "useOtherAccountToChangePassword": "false",
    "schema": "master"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

## **Add a UNIX Target Connector**

Use the UNIX target connector to manage UNIX-based privileged accounts. This connector uses either the SSH-2 or Telnet protocol for communication.

To add the target connector using the CLI, see [UNIX Target Connector CLI Configuration](#).

To add the target connector using the external API, see [UNIX Target Connector External API Configuration](#).

## **Add the Target Application and Connector**

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name:** Select the magnifying glass to pick the target server
  - **Device Name**
  - **Application Name:** Application names must be unique for a given target server.
4. In the **Application Type** field, select UNIX.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select the tab for the access communication method you are using (SSH-2 or Telenet) and fill-in the required fields.

### **SSH-2 Tab - Connection information**

- **Port:** Enter the port that connects to the Cisco host using SSH.
- **Communication Timeout:** Specify the amount of time the appliance waits for communication from the remote target server before ending the connection.
- **SSH Key Pair Policy:** Select the key pair that secures the connection. For more information, see [Create an SSH Key Pair Policy with the UI](#).
- **SSH Certificate Policy:** Select the certificate that secures the connection. For more information, see [Create an SSH Certificate Policy with the UI](#).
- **Enable strict host key checking:** Select this checkbox to control whether a system whose host key is unknown or whose key changed gets automatically added to the known host list. Provide the Known Host Key or the Known Host Key Fingerprint so the host can be verified

### **SSH-2 Tabs - Cipher, Hash, Key Exchange, Compression, Server Host Key**

Selecting the checkbox on each tab results in the appliance using the supported settings for each feature. Clearing the checkbox displays more settings, letting you customize how the appliance handles the SSH-2 features.

- **Cipher:** Select the checkbox to use supported ciphers. Clear the checkbox to reveal fields for entering a list of inbound and outbound ciphers.
- **Hash:** Specifies whether the supported hashes should be used when making an SSH connection to the remote host. Clear the checkbox to reveal fields for entering a list of inbound and outbound hashes.
- **Key Exchange:** Select the checkbox to use supported key exchange methods. Clear the checkbox to reveal fields for entering a list of key exchange methods.
- **Compression:** Select the checkbox to use supported compression methods. Clear the checkbox to reveal fields for entering a list of inbound and outbound compression methods.
- **Server Host Key:** Select the checkbox to use supported server host key types. Clear the checkbox to reveal fields for entering a list of server host key types.

### **NOTE**

Encryption standards continue to evolve with new vulnerabilities identified in what were previously accepted algorithms. Progress is also made with additional more-secure Cipher, Hash, Key Exchange, or Server Host Key options added to common utilities used for establishing secure communication channels. When upgrading PAM, be sure to consider any changes in the available more-secure cipher algorithms. Less secure Ciphers, Hashes, Key Exchanges, or Server Host Keys algorithms are not listed, but will continue working but may be subject to removal in a future release.

## 7. Telnet Tab

- **Port:** Enter the port that the appliance uses to connect to the UNIX host with Telnet. Default: 23
- **Communication Timeout:** Specify the amount of time, in milliseconds, that the appliance waits for communication from the remote target server. If the remote host does not respond when the time expires, the appliance ends the connection. Default: 60000

8. Select **OK**.

## Use a Script to Simplify Communication (Optional)

The UNIX target connector includes a large amount of low-level code to handle communications with the remote host. Credential Manager can use a script processor to simplify such communications.

The script processor (written in Java) executes a high-level version of the logic for manipulating credentials on remote hosts. Two scripts allow different levels of testing and production use. One script verifies passwords while the other script updates passwords.

A set of default scripts that is provided with the appliance. To use the default scripts, configure a set of default prompts and command values.

When adding target applications and target accounts, you can configure the script settings with the UI or the CLI.

### Generate the Script

Follow these steps to generate the script:

1. Select the **Script Processor** tab.
2. Complete the following fields:
  - **UNIX Variant:** Select the type of UNIX system that is installed on the target server. This option adapts the connection script that is used to that version. If the UNIX type is unknown, select Generic. If the type is known but not listed, select Other.
  - **Script Timeout:** (optional) Enter the amount of time (5000 through 59999 milliseconds), that the appliance waits to receive expected input from the remote host. Default: 5000
3. Optionally, specify regular expressions for the script variables. When specified, the following prompts and commands are substituted into appropriate variables in the default scripts. You can enter a substitute string.  
The following table lists the various prompts:

Prompt	Expression
Password Change Prompt	This regular expression matches the prompt that from the remote host when it requests a password change due to expiration. Default: (?si).*?change your password.*?
Password Confirmation Prompt	This regular expression matches the prompt from the remote host when it requests a password confirmation. Default: (?si).*?password:.*?
Password Entry Prompt	This regular expression matches the prompt from by the remote host when it requests a password. Default: (?si)(.*?password(\sfor :).*)?
User Name Entry Prompt	This regular expression matches the prompt from the remote host when it requests a user name.Default: (?si).*?login:.*?
Change File Permissions Command	The command on the remote host that changes file permissions. Default: chmod
Change Password Command	The command on the remote host that changes a password. Default: passwd



Echo Command	The command on the remote host that repeats a sequence of characters to the standard output, that is, the console. Default: <code>echo</code>
Pattern Matching Command	The command on the remote host that is used for pattern matching. Default: <code>grep</code>
Policy Management Command	The command on the remote host that manages policy. Default on AIX: <code>pwdadm</code> Default on any other platform: (none)
Privilege Elevation Command	The command on the remote host that elevates the level of privilege. Default: <code>sudo</code>
Substitute User Command	The command on the remote host that acts as another user. Default: <code>su</code>
System Information Command	Default: <code>uname</code>
Who Am I Command	The command on the remote host that is used to retrieve the effective ID of the currently logged-in user. Default: <code>whoami</code>
Exit Status of Last Command	Default: <code>\$?</code> To use <code>csch</code> on AIX, set this value to <code>"\$status"</code> .

### ***Apply the Script to Update and Verify Credentials***

#### **Follow these steps:**

1. Select the **Credentials Script** tab.
2. In the Update and Verify sections, select one of the available options:

#### **TIP**

We recommend that you use the default script. If a revised script is required, contact CA Services.

#### **NOTE**

For the script to work properly, the alias for the UNIX commands must be commented in the `.bashrc` file for that account. If you plan to use an alias, please contact Broadcom services to get a revised script.

3. – **Use the default script**  
Select this option for the appliance to use the default script that is provided with the release. If changes to the script logic are required, contact CA Services.
- **Use a revised default script (requires patch)**  
Select this option to use a revised script that is provided by CA Services. Select the appropriate script from the drop-down list.
- **Use a replacement script**  
Select this option to use a replacement script. When selected, this option opens the **Replacement Script** text box. Paste the new script in the box, and try the operation.  
You might have to try more than one replacement script so the appliance conforms to your OS environment. Only edit the replacement scripts with assistance from CA Services.

#### **WARNING**

**Customer Responsibilities for Custom Scripts:** If you build custom scripts, you are responsible for the operation between the target application and the target endpoint. CA Technologies is responsible for operation up to the point where PAM passes information to the custom target application. After that point, you are responsible for how the custom script handles communication at an operational and security level.

### Specify Account Discovery Criteria for the Server (Optional)

To simplify adding target accounts for a given server and application, you can use account discovery to find accounts. The settings on this tab let you specify the criteria that the appliance uses to determine a privileged account. To limit the accounts that Account Discovery returns, select the **UID** (User ID) or the **GID** (group ID). Enter a single ID or a range of values. For the account to be discovered, the account must satisfy *both* criteria.

#### NOTE

Next Step: [Add a target account to the target application.](#)

## UNIX Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding a UNIX target applications and target accounts.

### UNIX Target Connector CLI Parameters

To add a UNIX target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	unixII

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
no	N/A	unixII

#### ***Attribute.sshPort***

The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### ***Attribute.sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.sshKeyPairPolicyID***

Specifies the SSH Key Policy ID which controls how keys are generated; that is, the key type (ECDSA or RSA or DSA) and length.

Required	Default Value	Valid Values
no	N/A	0-9

**Attribute.sshStrictHostKeyCheckingEnabled**

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Required	Default Value	Valid Values
no	false	true, false

**Attribute.sshKnownHostKey**

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

**Attribute.sshKnownHostKeyFingerprint**

Contains the fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is for display purposes only. It allows the user to easily compare one key with another. The fingerprint that is specified must correspond to the specified public host key.

Required	Default Value	Valid Values
no	N/A	a public key fingerprint

**Attribute.sshUseDefaultCiphers**

Specifies whether the default ciphers should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

**Attribute.sshServerToClientCiphersList**

Specifies the list of ciphers to accept on the inbound data stream from the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

**Attribute.sshClientToServerCiphersList**

Specifies the list of ciphers to use on the outbound data stream to the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

#### ***Attribute.sshDetectCiphersList***

Specifies the list of ciphers to detect when connecting to the remote host. Credential Manager does not use ciphers that are unavailable even if they are specified to use as inbound and/or outbound ciphers. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

#### ***Attribute.sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerToClientHashesList***

Specifies the list of hashes to accept on the inbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

#### ***Attribute.sshClientToServerHashesList***

Specifies the list of hashes to accept on the outbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

#### ***Attribute.sshUseDefaultKeyExchangeAlgorithms***

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshKeyExchangeAlgorithmsList***

Specifies the list of key exchange methods to use when connecting to the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if sshUseDefaultKeyExchangeAlgorithms is false	diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1	A comma-separated list containing one or more of the following values: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1. Do not use spaces in the list.

#### ***Attribute.sshUseDefaultCompressionAlgorithms***

Specifies whether the default compression methods are used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerToClientCompressionAlgorithmsList***

Specifies the list of compression methods to accept on the inbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if sshUseDefaultCompressionAlgorithms is false	N/A. Do not use compression	comma-separated list containing one or more of the following values: zlib, zlib@openssh.com. Do not use spaces in the list.

#### ***Attribute.sshClientToServerCompressionAlgorithmsList***

Specifies the list of compression methods to use on the outbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
Yes if sshUseDefaultCompressionAlgorithms is false	N/A (do not use compression)	A comma-separated list containing one or more of the following values: zlib, zlib@openssh.com. Do not use spaces in the list.

#### ***Attribute.sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

#### ***Attribute.sshServerHostKeyAlgorithmsList***

Specifies the list of host key types to accept when Credential Manager connects to the remote host.

Required	Default Value	Valid Values
yes if sshUseDefaultServerHostKeyAlgorithms is false	ssh-rsa,ssh-dss	A comma-separated list containing one or more of the following values: ssh-rsa, ssh-dss. Do not use spaces in the list.

#### ***Attribute.telnetSessionTimeout***

When using the Telnet communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.telnetPort***

The port that is used to connect to the UNIX host using Telnet.

Required	Default Value	Valid Values
no	23	0-65536

#### ***Attribute.scriptTimeout***

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

#### ***Attribute.unixVariant***

Specifies the type of UNIX system that is installed on the target server.

Required	Default Value	Valid Values
no	GENERIC	AIX, GENERIC, HPUX, LINUX, SOLARIS or OTHER.

#### ***Attribute.useUpdateScriptType***

Specifies whether the default, revised, or replacement update script should be used. If a revised script is required, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### ***Attribute.revisedUpdateScriptFilename***

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

#### ***Attribute.useVerifyScriptType***

Specifies whether the default, revised or replacement verify that script should be used. If a revised script is required, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

#### ***Attribute.revisedVerifyScriptFilename***

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

#### ***Attribute.userNameEntryPrompt***

A regular expression that matches the prompt of the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

#### ***Attribute.passwordEntryPrompt***

A regular expression that matches the prompt of the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si).*(password(\sfor :).*)	valid regular expression syntax

#### ***Attribute.passwordConfirmationPrompt***

A regular expression that matches the prompt from the remote host when it requests that a password be confirmed.

Required	Default Value	Valid Values
no	AIX: (?si).*(new password.*? All other platforms: (?si).*(password:.*?)	valid regular expression syntax

***Attribute.passwordChangePrompt***

A regular expression that matches the prompt of the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*?change your password.*?	valid regular expression syntax

***Attribute.changePasswordCommand***

The command on the remote host that is used to change a password.

Required	Default Value	Valid Values
no	passwd	depends on remote host

***Attribute.elevatePrivilegeCommand***

The command on the remote host that is used to elevate the user's level of privilege.

Required	Default Value	Valid Values
no	sudo	depends on remote host

***Attribute.substituteUserCommand***

The command on the remote host that is used to act as another user.

Required	Default Value	Valid Values
no	su	depends on remote host

***Attribute.echoCommand***

The command on the remote host that is used to repeat a sequence of characters to the standard output; that is, the console.

Required	Default Value	Valid Values
no	echo	depends on remote host

***Attribute.patternMatchingCommand***

The command on the remote host that prints lines matching a pattern.

Required	Default Value	Valid Values
no	grep	depends on remote host

***Attribute.policyManagementCommand***

The command on the remote host that is used to manage policy.

Required	Default Value	Valid Values
no	AIX: pwdadm All other platforms: N/A	depends on remote host



**Attribute.whoAmICommand**

The command on the remote host that is used to retrieve the effective ID of the currently logged-in user.

Required	Default Value	Valid Values
no	whoami	depends on remote host

**Attribute.changeFilePermissionsCommand**

The command on the remote host that is used to alter the permissions on a file.

Required	Default Value	Valid Values
no	chmod	depends on remote host

**UNIX Target Account CLI Parameters**

To add a UNIX target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

**Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

**Attribute.otherAccount**

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

**Attribute.verifyThroughOtherAccount**

Specifies whether the credentials of a second target account are used to authenticate to the remote host when verifying the target account.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is true.	false	true, false

**Attribute.passwordChangeMethod**

Specifies which method to use when updating passwords. You might need to select a method that enables the authenticated user to obtain greater privileges without being impacted by policies at the remote host, such as the minimum length of time between password updates.

Required	Default Value	Valid Values
yes if <code>Attribute.useOtherAccountToChangePassword</code> is false.	DO_NOT_USE_SUDO	DO_NOT_USE_SUDO, USE_SUDO, IS_ROOT_ACCOUNT, USE_AUTHENTICATED_SUDO

### ***Attribute.protocol***

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH, SSH2_PUBLIC_KEY_AUTH, TELNET

### ***Attribute.passphrase***

The passphrase that protects the private key.

Required	Default Value	Valid Values
no	N/A	a string

### ***Attribute.publicKey***

Specifies the public key that corresponds to the target account private key. The private key is stored as its password.

Required	Default Value	Valid Values
yes if the select protocol is <code>SSH2_PUBLIC_KEY_AUTH</code>	N/A	an OpenSSH-formatted public key

### ***Attribute.keyOptions***

Specifies a list of comma-separated option specifications from the `authorized_keys` file format that is described in the OpenSSH documentation.

Required	Default Value	Valid Values
no	N/A	comma-separated list of OpenSSH key options

### **UNIX CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=www.ca.com
TargetApplication.type=unixII TargetApplication.name=UNIX
Attribute.extensionType=unixII Attribute.useDefaultUpdateScript=true
Attribute.useDefaultVerifyScript=true Attribute.unixVariant=GENERIC
```

```
cmdName=addTargetAccount TargetServer.hostName=www.ca.com TargetApplication.name=UNIX
TargetAccount.userName=account1
```

```
TargetAccount.password=password1 Attribute.protocol=SSH2_PASSWORD_AUTH
Attribute.useOtherAccountToChangePassword=false
Attribute.passwordChangeMethod=DO_NOT_USE_SUDO
```

## UNIX Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a UNIX (aka UNIXII) Target Application using the External API.

### UNIX Target Application External API Attributes

To add or update a UNIX Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

Required	Default Value	Valid Values
no	N/A	unixII

#### ***sshPort***

The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### ***sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***sshKeyPairPolicyID***

Specifies the SSH Key Policy ID which controls how keys are generated; that is, the key type (ECDSA or RSA or DSA) and length.

Required	Default Value	Valid Values
no	N/A	0-9

#### ***sshStrictHostKeyCheckingEnabled***

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Required	Default Value	Valid Values
no	false	true, false

***sshKnownHostKey***

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

***sshKnownHostKeyFingerprint***

Contains the fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is for display purposes only. It allows the user to easily compare one key with another. The fingerprint that is specified must correspond to the specified public host key.

Required	Default Value	Valid Values
no	N/A	a public key fingerprint

***sshUseDefaultCiphers***

Specifies whether the default ciphers should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

***sshServerToClientCiphersList***

Specifies the list of ciphers to accept on the inbound data stream from the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

***sshClientToServerCiphersList***

Specifies the list of ciphers to use on the outbound data stream to the remote host. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

***sshDetectCiphersList***

Specifies the list of ciphers to detect when connecting to the remote host. Credential Manager does not use ciphers that are unavailable even if they are specified to use as inbound and/or outbound ciphers. Ciphers are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCiphers</code> is false	aes128-ctr,aes128-cbc,3des-ctr,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc	A comma-separated list containing one or more of the following values: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-ctr, arcfour, arcfour128, arcfour256. Do not use spaces in the list.

### ***sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

### ***sshServerToClientHashesList***

Specifies the list of hashes to accept on the inbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

### ***sshClientToServerHashesList***

Specifies the list of hashes to accept on the outbound data stream from the remote host. Hashes are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultHashes</code> is false	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

### ***sshUseDefaultKeyExchangeAlgorithms***

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

### ***sshKeyExchangeAlgorithmsList***

Specifies the list of key exchange methods to use when connecting to the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultKeyExchangeAlgorithms</code> is false	<code>diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1</code>	A comma-separated list containing one or more of the following values: <code>diffie-hellman-group1-sha1</code> , <code>diffie-hellman-group14-sha1</code> , <code>diffie-hellman-group-exchange-sha1</code> . Do not use spaces in the list.

### ***sshUseDefaultCompressionAlgorithms***

Specifies whether the default compression methods are used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

### ***sshServerToClientCompressionAlgorithmsList***

Specifies the list of compression methods to accept on the inbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A. Do not use compression	comma-separated list containing one or more of the following values: <code>zlib</code> , <code>zlib@openssh.com</code> . Do not use spaces in the list.

### ***sshClientToServerCompressionAlgorithmsList***

Specifies the list of compression methods to use on the outbound data stream from the remote host. Methods are listed in order of priority.

Required	Default Value	Valid Values
Yes if <code>sshUseDefaultCompressionAlgorithms</code> is false	N/A (do not use compression)	A comma-separated list containing one or more of the following values: <code>zlib</code> , <code>zlib@openssh.com</code> . Do not use spaces in the list.

### ***sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host.

Required	Default Value	Valid Values
no	true	true, false

### ***sshServerHostKeyAlgorithmsList***

Specifies the list of host key types to accept when Credential Manager connects to the remote host.

Required	Default Value	Valid Values
yes if sshUseDefaultServerHostKeyAlgorithms is false	ssh-rsa,ssh-dss	A comma-separated list containing one or more of the following values: ssh-rsa, ssh-dss. Do not use spaces in the list.

### ***telnetSessionTimeout***

When using the Telnet communication channel, specifies the amount of time in milliseconds that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

### ***telnetPort***

The port that is used to connect to the UNIX host using Telnet.

Required	Default Value	Valid Values
no	23	0-65536

### ***scriptTimeout***

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

### ***unixVariant***

Specifies the type of UNIX system that is installed on the target server.

Required	Default Value	Valid Values
no	GENERIC	AIX, GENERIC, HPUX, LINUX, SOLARIS or OTHER.

### ***useUpdateScriptType***

Specifies whether the default, revised, or replacement update script should be used. If a revised script is required, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

### ***revisedUpdateScriptFilename***

Specifies the name of the file containing the revised update script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

### ***useVerifyScriptType***

Specifies whether the default, revised or replacement verify that script should be used. If a revised script is required, use the default script and contact CA Services.

Required	Default Value	Valid Values
no	'DEFAULT'	'DEFAULT', 'REVISED' or 'REPLACEMENT'

### ***revisedVerifyScriptFilename***

Specifies the name of the file containing the revised verify script. The contents of the file is used as the revised script. We recommend that you use the default script and contact CA Services if a revised script is required.

Required	Default Value	Valid Values
no	N/A	a file name

### ***userNameEntryPrompt***

A regular expression that matches the prompt of the remote host when it requests a user name.

Required	Default Value	Valid Values
no	(?si).*(login username):.*?	valid regular expression syntax

### ***passwordEntryPrompt***

A regular expression that matches the prompt of the remote host when it requests a password.

Required	Default Value	Valid Values
no	(?si).*(password (?for :)).*?	valid regular expression syntax

### ***passwordConfirmationPrompt***

A regular expression that matches the prompt from the remote host when it requests that a password be confirmed.

Required	Default Value	Valid Values
no	AIX: (?si).*(new password).*? All other platforms: (?si).*(password:.*?)	valid regular expression syntax

### ***passwordChangePrompt***

A regular expression that matches the prompt of the remote host when it requests that a password be changed because it has expired.

Required	Default Value	Valid Values
no	(?si).*(change your password).*?	valid regular expression syntax



***changePasswordCommand***

The command on the remote host that is used to change a password.

Required	Default Value	Valid Values
no	passwd	depends on remote host

***elevatePrivilegeCommand***

The command on the remote host that is used to elevate the user's level of privilege.

Required	Default Value	Valid Values
no	sudo	depends on remote host

***substituteUserCommand***

The command on the remote host that is used to act as another user.

Required	Default Value	Valid Values
no	su	depends on remote host

***echoCommand***

The command on the remote host that is used to repeat a sequence of characters to the standard output; that is, the console.

Required	Default Value	Valid Values
no	echo	depends on remote host

***patternMatchingCommand***

The command on the remote host that prints lines matching a pattern.

Required	Default Value	Valid Values
no	grep	depends on remote host

***policyManagementCommand***

The command on the remote host that is used to manage policy.

Required	Default Value	Valid Values
no	AIX: pwdadm All other platforms: N/A	depends on remote host

***whoAmICommand***

The command on the remote host that is used to retrieve the effective ID of the currently logged-in user.

Required	Default Value	Valid Values
no	whoami	depends on remote host

***changeFilePermissionsCommand***

The command on the remote host that is used to alter the permissions on a file.

Required	Default Value	Valid Values
no	chmod	depends on remote host

### **UNIX Target Account External API Attributes**

To add a UNIX target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account when updating the target account.

Required	Default Value	Valid Values
yes	false	true, false

#### ***otherAccount***

Specifies which other account to use when updating the target account.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	N/A	a valid target account ID.

#### ***verifyThroughOtherAccount***

Specifies whether the credentials of a second target account are used to authenticate to the remote host when verifying the target account.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is true.	false	true, false

#### ***passwordChangeMethod***

Specifies which method to use when updating passwords. You might need to select a method that enables the authenticated user to obtain greater privileges without being impacted by policies at the remote host, such as the minimum length of time between password updates.

Required	Default Value	Valid Values
yes if <code>useOtherAccountToChangePassword</code> is false.	DO_NOT_USE_SUDO	DO_NOT_USE_SUDO, USE_SUDO, IS_ROOT_ACCOUNT, USE_AUTHENTICATED_SUDO

#### ***protocol***

Specifies the protocol to use for communicating with the remote host.

Required	Default Value	Valid Values
yes if useOtherAccountToChangePassword is false	SSH2_PASSWORD_AUTH	SSH2_PASSWORD_AUTH, SSH2_PUBLIC_KEY_AUTH, TELNET

### ***passphrase***

The passphrase that protects the private key.

Required	Default Value	Valid Values
no	N/A	a string

### ***publicKey***

Specifies the public key that corresponds to the target account private key. The private key is stored as its password.

Required	Default Value	Valid Values
yes if the select protocol is SSH2_PUBLIC_KEY_AUTH	N/A	an OpenSSH-formatted public key

### ***keyOptions***

Specifies a list of comma-separated option specifications from the authorized\_keys file format that is described in the OpenSSH documentation.

Required	Default Value	Valid Values
no	N/A	comma-separated list of OpenSSH key options

## **UNIX (UNIXII) Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "UnixApp",
  "applicationType": "unixII",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "passwordEntryPrompt": "",
    "sshSessionTimeout": "",
    "echoCommand": "",
    "telnetSessionTimeout": "",
    "useUpdateScriptType": "DEFAULT",
    "substituteUserCommand": "",
    "acctDiscGidValue": "",
    "acctDiscUidRangeLow": "",
    "acctDiscGidRangeLow": "",
    "sshUseDefaultKeyExchangeAlgorithms": "true",
    "sshKeyPairPolicyID": "",
  }
}
```

```

    "acctDiscUidValue": "",
    "passwordConfirmationPrompt": "",
    "changeFilePermissionsCommand": "",
    "sshPort": "",
    "changePasswordCommand": "",
    "useVerifyScriptType": "DEFAULT",
    "sshServerToClientCiphersList": "",
    "elevatePrivilegeCommand": "",
    "sshKnownHostKey": "",
    "sshKnownHostKeyFingerprint": "",
    "exitStatusOfLastCommand": "",
    "sshServerToClientCompressionAlgorithmsList": "",
    "extensionType": "unixII",
    "systemInfoCommand": "",
    "patternMatchingCommand": "",
    "acctDiscGidRangeHigh": "",
    "acctDiscGidType": "",
    "sshDetectCiphersList": "",
    "sshClientToServerCiphersList": "",
    "sshClientToServerCompressionAlgorithmsList": "",
    "passwordChangePrompt": "",
    "acctDiscUidType": "",
    "acctDiscUidRangeHigh": "",
    "sshUseDefaultCiphers": "true",
    "sshServerHostKeyAlgorithmsList": "",
    "userNameEntryPrompt": "",
    "sshUseDefaultHashes": "true",
    "unixVariant": "GENERIC",
    "whoAmICommand": "",
    "telnetPort": "",
    "sshKeyExchangeAlgorithmsList": "",
    "policyManagementCommand": "",
    "sshUseDefaultCompressionAlgorithms": "true",
    "acctDiscUseUid": "f",
    "sshUseDefaultServerHostKeyAlgorithms": "true",
    "scriptTimeout": "",
    "sshClientToServerHashesList": "",
    "sshServerToClientHashesList": "",
    "sshStrictHostKeyCheckingEnabled": "false",
    "acctDiscUseGid": "false"
  },
  "passwordCompositionPolicyId": null
}

```

**UNIX (UNIXII) Target Account External API Example**

POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/  
targetAccounts

```
{
  "accountName": "UnixAcc",
  "attributes": {
    "keyOptions": "",
    "verifyThroughOtherAccount": "false",
    "discoveryAllowed": "f",
    "privateKey": "",
    "protocol": "SSH2_PASSWORD_AUTH",
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "useOtherAccountToChangePassword": "false",
    "passwordChangeMethod": "DO_NOT_USE_SUDO"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

**Add a VMware ESX/ESXi Target Connector**

Use this VMware ESX/ESXi connector to synchronize passwords of ESX/ESXi target accounts. This target connector uses WSDL over SSL.

To add the target connector using the CLI, see [VMware ESX/ESXi CLI Target Configuration](#).

To add the target connector using the external API, see [VMware ESX/ESXi Target Connector External API Configuration](#).

**Add the Target Application and Connector**

**Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **VMware ESX/ESXi**.
5. (Optional) Select a password composition policy.

If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.

6. Select the VMware ESX/ESXi tab and specify the SSL port. The default is 443.
7. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application.](#)

## VMware ESX/ESXi Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding a VMware ESX/ESXi target application and target account:

### VMware ESX/ESXi Target Application CLI Parameters

To add a ESX/ESXi target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	vmware

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	vmware

#### ***Attribute.sslPort***

The target application port.

Required	Default Value	Valid Values
yes	443	0-65535

### VMware ESX/ESXi Target Account CLI Parameters

To add a target account that uses the VMWARE ESX/ESXi target connector, use the [addTargetAccount](#) command and the following command parameters:

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
yes	N/A	vmware

#### ***Attribute.useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.otherAccount**

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes Attribute.useOtherAccountToChangePassword is true.	N/A	A valid target account ID.

**VMware ESX/ESXi CLI Example**

```
cmdName=addTargetApplication
  TargetServer.hostName=myhostname.mydomain.com TargetApplication.name=myESXi

TargetApplication.type=vmware Attribute.extensionType=vmware Attribute.sslPort=443
```

```
cmdName=addTargetAccount
  TargetServer.hostName=myhostname.mydomain.com TargetApplication.name=myESXi

TargetAccount.userName=root TargetAccount.password=P@ssw0rd
  TargetAccount.cacheAllow=true

TargetAccount.cacheDuration=19 Attribute.extensionType=vmware
  Attribute.useOtherAccountToChangePassword=false
```

**VMware ESX/ESXi Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating a VMware ESX/ESXi Target Application using the External API.

**VMware ESX/ESXi Target Application External API Attributes**

To add or update a VMware ESX/ESXi Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

**extensionType**

Required	Default Value	Valid Values
yes	N/A	vmwa

**sslPort**

The target application port.

Required	Default Value	Valid Values
yes	443	0-65535

### **VMware ESX/ESXi Target Account External API Attributes**

To add a VMware ESX/ESXi target account that uses the target connector, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### ***extensionType***

Required	Default Value	Valid Values
yes	N/A	vmware

#### ***useOtherAccountToChangePassword***

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

#### ***otherAccount***

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
yes useOtherAccountToChangePassword is true.	N/A	A valid target account ID.

### **VMware ESX/ESXi Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "vmwareApp",
  "applicationType": "vmware",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "mbean": "",
    "instance": "",
    "port": "",
    "extensionType": "vmware",
    "sslEnabled": "",
    "sslPort": "443"
  },
  "passwordCompositionPolicyId": null
}
```

### **VMware ESX/ESXi Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/targetAccounts
```



```
{
  "accountName": "vmwareAcc95",
  "attributes": {
    "otherAccount": "",
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "discoveryAllowed": "f",
    "useOtherAccountToChangePassword": "false"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

**NOTE**

`useOtherAccountToChangePassword : "false"` false/true values only.

## Add a VMware NSX Controller Target Connector

**WARNING**

VMware NSX API support is deprecated and will be removed in a subsequent version of PAM.

Use the VMware NSX Controller target connector to provide synchronization support for NSX controller target accounts.

To add the target connector using the CLI, see [VMware NSX Controller CLI Target Connector](#).

To add the target connector using the external API, see [VMware NSX Controller Target Connector External API Configuration](#).

### Add the Target Application and Connector

#### Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **VMware NXS Controller**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select the **VMware NXS Controller** tab and specify the following settings:

- **Script Timeout:** Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host. Valid values are 5000-99999. Default: **5000**
- **Port:** If you are using an SSL connection, indicate the port that is used to connect to the UNIX host using SSH. Valid values are 0-65535. Default: 22
- **Communications Timeout:** If you are using an SSH connection, specify the amount of time in milliseconds that Credential Manager waits for the remote host to respond. Valid values are 1000-99999. Default: 5000

7. Select **OK** to save the changes.

#### NOTE

**Next Step:** [Add a target account to the target application.](#)

## VMware NSX Controller Target Connector CLI Configuration

This topic includes CLI commands and parameters for adding VMware NSX Controller target applications and target accounts:

### VMware NSX Controller Target Application CLI Parameters

To add a VMware NSX Controller target application and connector, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	nsxcontroller

#### ***Attribute.sshPort***

The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### ***Attribute.sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager waits for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.scriptTimeout***

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

## VMware NSX Controller Target Account CLI Parameters

When using the CLI to add a VMware NSX Controller target account, this target connector does not require any parameters.

### VMware NSX Controller CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myNXS
```

```
TargetApplication.type=nsxcontroller Attribute.extensionType=nsxcontroller
Attribute.sshPort=22
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myNSX
```

```
TargetAccount.userName=root TargetAccount.password=P@ssw0rd
TargetAccount.cacheAllow=true TargetAccount.cacheDuration=19
```

## VMware NSX Controller Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a VMware NSX Controller Target Application using the External API:

### VMware NSX Controller Target Application External API Attributes

To add or update a xxx Target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call:

#### **sshPort**

The port that is used to connect to the UNIX host using SSH.

Required	Default Value	Valid Values
no	22	0-65535

#### **sshSessionTimeout**

When using the SSH communication channel, specifies the amount of time in milliseconds that Credential Manager waits for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### **scriptTimeout**

Specifies the amount of time in milliseconds that Credential Manager waits to receive some expected input from the remote host.

Required	Default Value	Valid Values
no	5000	5000-59999

### **VMware NSX Controller Target Account External API Attributes**

When using the API to add a VMware NSX Controller target account, this target connector does not have any additional attributes.

### **VMware NSX Controller Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "NSXControllerApp",
  "applicationType": "nsxcontroller",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "attributes": {
    "sshPort": "",
    "scriptTimeout": "",
    "sshSessionTimeout": ""
  },
  "passwordCompositionPolicyId": null
}
```

### **VMware NSX Controller Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "nsxControllerAcc",
  "attributes": {
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "discoveryAllowed": "f"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

## Add a VMware NSX Proxy Target Connector

This target connector provides synchronization support for NSX proxy target accounts. Use this VMware NSX Proxy connector to synchronize passwords of NSX target accounts.

To add the target connector using the CLI, see [NSX Proxy Target Connector CLI Configuration](#).

To add the target connector using the external API, see [VMware NSX Proxy Target Connector External API Configuration](#).

### Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.
4. In the **Application Type** field, select **VMware NSX Proxy**.  
No VMware NSX Proxy tab displays; there are no settings to configure.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select **OK**.

#### NOTE

Next Step: [Add a target account to the target application](#).

## VMware NSX Proxy Target Connector CLI Configuration

For the NSX Proxy target connector, there are no additional parameters to add a target application or a target account.

### VMware NSX Proxy CLI Example

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myESXi
```

```
TargetApplication.type=nsxproxy Attribute.extensionType=nsxproxy
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myNSX_Proxy
```

```
TargetAccount.userName=root TargetAccount.password=P@ssw0rd
TargetAccount.cacheAllow=true TargetAccount.cacheDuration=19
```

## VMware NSX Proxy Target Connector External API Configuration

For the NSX Proxy target application and account, there are no additional attributes to add a target application or a target account.

### **VMware NSX Proxy Target Application External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "NSXProxyApp",
  "applicationType": "nsxproxy",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "passwordCompositionPolicyId": null
}
```

### **VMware NSX Proxy Target Account External API Example**

```
POST /api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "nsxProxyAcc",
  "attributes": {
    "descriptor2": "",
    "discoveryGlobal": "f",
    "descriptor1": "",
    "discoveryAllowed": "f"
  },
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "sample",
  "passwordViewPolicyId": 1000,
  "privileged": "t",
  "synchronize": "f",
  "useAliasNameParameter": "f"
}
```

## **Add a WebLogic Target Connector**

This target connector provides password synchronization functionality for Oracle WebLogic v10 application servers.

To add the target connector using the CLI, see [WebLogic Target Connector CLI Configuration](#).

### **Add the Target Application and Connector**

**Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name. Select the magnifying glass to pick the target server
  - Device Name
  - Application Name. Application names must be unique for a given target server.

4. In the **Application Type** field, select **WebLogic**.
5. (Optional) Select a password composition policy.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions
6. On the WebLogic tab, configure the following fields:
  - **Server Port:** The port that connects to the WebLogic server. Valid values: 0-65535. Default value: 7001
  - **MBean:** Enter the object name of the *managed bean (MBean)*. An MBean is a *JavaBean* that provides a *Java Management Extensions (JMX)* interface. The format is *domain:key=property*.
7. Select **OK**.

**NOTE**

Next Step: [Add a target account to the target application.](#)

## WebLogic Target Connector CLI Configuration

This topic contains the parameters for adding WebLogic target applications and target accounts:

### WebLogic Target Application CLI Parameters

To add a WebLogic target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### **TargetApplication.type**

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	weblogic10

#### **Attribute.extensionType**

Required	Default Value	Valid Values
yes	N/A	weblogic10

#### **Attribute.port**

The port that is used to connect to the WebLogic server.

Required	Default Value	Valid Values
yes	N/A	0-65535

### WebLogic Target Account CLI Parameters

To add a WebLogic target account that uses the target connector, use the [addTargetAccount](#) command and the following command parameters:

#### **Attribute.extensionType**

Required	Default Value	Valid Values
yes	N/A	weblogic10

**Attribute.realm**

Required	Default Value	Valid Values
yes	N/A	valid realm name

**Attribute.useOtherAccountToChangePassword**

Specifies whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

**Attribute.otherAccount**

Specifies which other account to use to perform password change requests.

Required	Default Value	Valid Values
Yes, if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

**WebLogic CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=weblogic10
```

```
TargetApplication.type=weblogic10 Attribute.extensionType=weblogic10 Attribute.port=7001
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=weblogic10
```

```
TargetAccount.userName=admin TargetAccount.password=p@ssw0rd
TargetAccount.cacheAllow=true
```

```
TargetAccount.cacheDuration=21 Attribute.extensionType=weblogic10
Attribute.realm=myrealm
```

```
Attribute.useOtherAccountToChangePassword=false
```



## Add a Windows SSH Key Target Connector

Use the PAM Windows SSH Key target connector to manage local account credentials on Windows systems using key-based SSH authentication.

The PAM Windows SSH Key target connector provides a highly secure solution for managing local privileged credentials on supported SSH-enabled Windows systems.

### NOTE

For a list of Windows versions that support the Windows SSH Password target connectors, see [Supported Platforms](#).

### TIP

The following alternative Windows connectors are available:

- **Windows SSH Password Connector:** Manages local Windows account credentials using password-based SSH authentication (less secure, also requires supported, SSH-enabled target system).
- **Windows Remote Target Connector:** Manages local Windows account credentials using the Windows Remote Desktop Service API (less secure than either SSH connector).
- **Windows Proxy Connector:** Functions similar to the Windows Remote Connector but requires the connector to be installed on a remote server in your target domain.

To add the target connector using the CLI, see [Windows SSH Key Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Windows SSH Key Target Connector External API Configuration](#).

### IMPORTANT

Do not configure scheduled jobs that change more than one Windows SSH Key target account using the **Use Same Password For All** option. This is not a supported use case and will result in errors.

## Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name:** Select the magnifying glass to pick the target server.
  - **Device Name:** The name of the target server. Populated dynamically when you pick the target server.
  - **Application Name:** A unique application name for the specified target server.
4. In the **Application Type** field, select **Windows SSH Key**.
5. Select the **SSH Connection** tab and complete the following fields:
  - **Port:** Enter the port that connects to the Windows host using SSH. The default value is 22.
  - **Communication Timeout:** Specify the amount of time that PAM waits for communication from the Windows host before ending the connection (in ms). The default value is 60000.
  - **SSH Key Pair Policy:** Specify the SSH key policy PAM uses to generate SSH key pairs. The key policy specifies the characteristics for the key pair, specifically the cryptographic algorithm, and the key size. When you update the target account that uses the key pair, the appliance pushes the public key to the target device.  
To configure or edit an SSH key policy, see [Configure SSH Key Pair Policies](#).  
Select the key pair that secures the connection. For more information, see [Configure SSH Key Pair Policies](#).
  - **Enable strict host key checking** (Optional) Select this option to protect against man-in-the-middle attacks by validating an SSH host key from the target server (specified in the required **Known Host Key** field) when establishing a connection.

**NOTE**

If a man-in-the-middle attack occurs, the malicious server to which your connection is redirected does not have the same SSH host key as the intended server and the connection is rejected.

- **Known Host Key** (Required if strict host key checking is enabled): Specify the base64 host key value of one of the SSH host keys configured on the target server. For example:

```
AAAAC3NzaC11ZD11NTE5AAAAIGq3L+ECE5S8CUJyZ0jiXbZReY7G/boxDUMrYlhrlK9w
```

**NOTE**

To obtain an SSH host key, you can use the [ssh-keyscan](#) utility on the target device. For example, `ssh-keyscan 127.0.0.1 2>$null` returns the IP address, host Key type and base64 host key value for all configured SSH host keys.

- **SHA256 Fingerprint** (Optional, only applicable if **Enable strict host key checking** is enabled): Specify a SHA256 fingerprint generated from the SSH host key on the target server to confirm that the value that you entered in the **Known Host Key** field matches. If the values do not match, PAM displays a dialog with an error message like the following:

```
PAM-CF-0005: Failed to validate target connector attributes. PAM-WS- 0103:Host key fingerprint does not match computed fingerprint: VpszjfaB00J5N43NQsawv1DsdeXyTzAd1bWLCak6GZl=..
```

**NOTE**

To obtain a SHA256 fingerprint, you can use the [ssh-keyscan](#) utility on the target device. For example, `ssh-keyscan 127.0.0.1 2>$null | ssh-keygen -E md5 -lf -` returns all the configured SSH host Keys and their SHA256 fingerprints.

6. Optionally, use the **Ciphers**, **Hashes**, **Key Exchange Methods**, and **Server Host Key Types** tabs to configure specific encryption algorithms to use when making an SSH connection to the remote host.

**NOTE**

By default, a **Use supported...** option is set on each tab, configuring support for all available encryption algorithms, as shown in the following screenshot:

Application	SSH Connection	Cipher	Hash	Key Exchange	Server Host Key Type
Use supported ciphers: <input checked="" type="checkbox"/>					
Use aes128-gcm: <input type="checkbox"/>					
Use aes128-ctr: <input type="checkbox"/>					
Use aes128-cbc (non FIPS): <input type="checkbox"/>					
Use aes192-ctr (non FIPS): <input type="checkbox"/>					
Use aes192-cbc (non FIPS): <input type="checkbox"/>					
Use aes256-gcm: <input type="checkbox"/>					
Use aes256-ctr: <input type="checkbox"/>					
Use aes256-cbc: <input type="checkbox"/>					

**Important:** if you unset the **Use supported...** option, you *must* select at least one of the listed encryption algorithms.

- **Cipher Tab:** Unset the **Use supported ciphers** option to select specific ciphers.
- **Hash Tab:** Unset the **Use supported hashes** option to select specific hashes.
- **Key Exchange Tab:** Unset the **Use supported key exchange methods** option to select specific key exchange methods.
- **Server Host Key Type Tab:** Unset the **Use supported server host key types** option to select specific server host key types.

**NOTE**

Encryption standards continue to evolve with new vulnerabilities that are identified in what were previously accepted algorithms. Progress is also made with other more-secure cipher, hash, key exchange, or server host key options added to common utilities used for establishing secure communication channels. When upgrading PAM, be sure to consider any changes in the available more-secure cipher algorithms. Less secure ciphers, hashes, key exchanges, or server host keys algorithms are no longer listed, but continue working. However, they may be subject to removal in a future release.

7. Select **OK**.

**NOTE**

**Next Step:** [Add a Windows SSH Key target account.](#)

## Windows SSH Key Target Connector CLI Configuration

This topic contains the CLI parameters for adding a Windows SSH Key target application and target account:

### Windows SSH Key Target Connector CLI Parameters

To add a Windows SSH Key target application using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	windowsSshKey

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
no	N/A	windowsSshKey

#### ***Attribute.sshPort***

The TCP port used to connect to the Windows host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

#### ***Attribute.sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds, that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	60000	1000-99999

#### ***Attribute.sshKeyPairPolicyID***

Specifies the SSH Key Policy ID which controls how keys are generated; that is, the key type (ECDSA or RSA or DSA) and length.

Required	Default Value	Valid Values
no	N/A	Integer that matches the ID of the required SSH Key Pair Policy.

#### ***Attribute.sshStrictHostKeyCheckingEnabled***

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Strict host key checking helps to provide protection from man-in-the-middle attacks. If such an attack happens, the malicious server you are redirected to would not have the same SSH host keys as the intended server. Thus attempts to connect to such a server would fail with strict host key checking.

Required	Default Value	Valid Values
no	false	true, false

#### ***Attribute.sshKnownHostKey***

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

#### ***Attribute.sshKnownHostKeyFingerprint***

Contains the SHA-256 fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint that is specified must correspond to the specified public host key. This attribute is optional when you specify a Known Host Key. Specifying this attributes value can help you ensure that you did not make a typographical error entering the Known Host Key.

Required	Default Value	Valid Values
no	N/A	a valid public key fingerprint

#### ***Attribute.sshUseDefaultCiphers***

Specifies the default ciphers to used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported ciphers, ignoring the setting to use specific ciphers. When set to false, Credential Manager only uses the selected ciphers.

Required	Default Value	Valid Values
no	true	true, false

### ***Ciphers That Support FIPS***

The following list displays the cipher algorithms that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useCipher_aes128-gcm</li> <li>Attribute.useCipher_aes128-ctr</li> <li>Attribute.useCipher_aes256-gcm</li> <li>Attribute.useCipher_aes256-ctr</li> <li>Attribute.useCipher_aes256-cbc</li> </ul>	no	false	true, false

### ***Ciphers That Do NOT Support FIPS***

The following list includes the algorithms that use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useCipher_aes128-cbc</li> <li>Attribute.useCipher_aes192-ctr</li> <li>Attribute.useCipher_aes192-cbc</li> </ul>	no	false	true, false

### ***Attribute.sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported hashes and ignores the setting to use specific hashes. When set to false, Credential Manager only uses the selected hashes.

Required	Default Value	Valid Values
no	true	true, false

### ***Hashes That Support FIPS***

The following list displays the hashes that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useHash_hmac-sha2-256</li> <li>Attribute.useHash_hmac-sha2-512</li> </ul>	no	false	true, false

### ***Hashes That Do NOT Use FIPS***

The following hash uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
Attribute.useHash_hmac-sha1	no	false	true, false

**Attribute.sshUseDefaultKeyExchangeAlgorithms**

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported key exchange methods, and ignore the setting to use specific key exchange methods. When set to false, the Credential Manager only uses the selected key exchange methods.

Required	Default Value	Valid Values
no	true	true, false

**These Key Exchange Methods Support FIPS**

The following list of displays the Key Exchange Methods that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useKeyExchange_curve25519-sha256</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp384</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp256</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp521</li> <li>Attribute.useKeyExchange_diffie-hellman-group14-sha1</li> <li>Attribute.useKeyExchange_diffie-hellman-group16-sha512</li> <li>Attribute.useKeyExchange_diffie-hellman-group18-sha512</li> <li>Attribute.useKeyExchange_diffie-hellman-group-exchange-sha256</li> </ul>	no	false	true, false

**These Key Exchange Methods Do NOT Support FIPS**

The following Key Exchange Methods use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useKeyExchange_curve25519-sha256</li> <li>Attribute.useKeyExchange_diffie-hellman-group14-sha256</li> </ul>	no	true	true, false

**Attribute.sshUseDefaultServerHostKeyAlgorithms**

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported server host key types, and ignore the setting to use specific ones. When set to false, the Credential Manager uses only the selected server host key types.

Required	Default Value	Valid Values
no	true	true, false

**These Host Key Types Support FIPS**

The following list displays the Host Key Types that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp384</li> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp256</li> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp521</li> <li>Attribute.useHostKeyType_rsa-sha2-512</li> <li>Attribute.useHostKeyType_rsa-sha2-256</li> <li>Attribute.useHostKeyType_ssh-rsa</li> </ul>	no	false	true, false

### ***These Host Key Types Do NOT Support FIPS***

The following Host Key Type uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
Attribute.useHostKeyType_ssh-ed25519	no	false	true, false

### **Windows SSH Key Target Application CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName={host name} TargetApplication.type=windowsSshKey
"TargetApplication.name=Windows SSH Key App" Attribute.sshPort=22
```

### **Windows SSH Key Target Account CLI Example**

```
cmdName=addTargetAccount TargetServer.hostName={hostname} "TargetApplication.name=Windows SSH Key App"
TargetAccount.privileged=true TargetAccount.synchronize=false TargetAccount.userName=WinSshKeyAct
TargetAccount.password=_generate_pass_ Attribute.changePasswordAccount={other account id}
Attribute.changeProcess=CHANGE_PROCESS_USE_DIFFERENT_ACCOUNT_TO_CHANGE_PASSWORD
```

## **Windows SSH Key Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating a Windows SSH Key target application using the External API.

### **Windows SSH Key Target Application External API Attributes**

To add or update a Windows SSH Key target application, use the following properties as members of the `attributes` associative array included in the `body` parameter of the `/api.php/v1/devices.json/{id}/targetApplications` External API method:

:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	windowsSshKey

**extensionType**

Required	Default Value	Valid Values
no	N/A	windowsSshKey

**sshPort**

The TCP port used to connect to the Windows host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

**sshSessionTimeout**

When using the SSH communication channel, specifies the amount of time in milliseconds, that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	60000	1000-99999

**sshKeyPairPolicyID**

Specifies the SSH Key Policy ID which controls how keys are generated; that is, the key type (ECDSA or RSA) and length.

Required	Default Value	Valid Values
no	N/A	Integer that matches the ID of the required SSH Key Pair Policy.

**sshStrictHostKeyCheckingEnabled**

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Strict host key checking helps to provide protection from man-in-the-middle attacks. If such an attack happens, the malicious server you are redirected to would not have the same SSH host keys as the intended server. Thus attempts to connect to such a server would fail with strict host key checking.

Required	Default Value	Valid Values
no	false	true, false

**sshKnownHostKey**

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

**sshKnownHostKeyFingerprint**



Contains the SHA-256 fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint that is specified must correspond to the specified public host key. This attribute is optional when you specify a Known Host Key. Specifying this attributes value can help you ensure that you did not make a typographical error entering the Known Host Key.

Required	Default Value	Valid Values
no	N/A	a valid public key fingerprint

### ***sshUseDefaultCiphers***

Specifies the default ciphers to used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported ciphers, ignoring the setting to use specific ciphers. When set to false, Credential Manager only uses the selected ciphers.

Required	Default Value	Valid Values
no	true	true, false

### ***Ciphers That Support FIPS***

The following list displays the cipher algorithms that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useCipher_aes128-gcm</li> <li>useCipher_aes128-ctr</li> <li>useCipher_aes256-gcm</li> <li>useCipher_aes256-ctr</li> <li>useCipher_aes256-cbc</li> </ul>	no	false	true, false

### ***Ciphers That Do NOT Support FIPS***

The following list includes the algorithms that use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useCipher_aes128-cbc</li> <li>useCipher_aes192-ctr</li> <li>useCipher_aes192-cbc</li> </ul>	no	false	true, false

### ***sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported hashes and ignores the setting to use specific hashes. When set to false, Credential Manager only uses the selected hashes.

Required	Default Value	Valid Values
no	true	true, false

### ***Hashes That Support FIPS***

The following list displays the hashes that support FIPS:

Hash Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useHash_hmac-sha2-256</li> <li>useHash_hmac-sha2-512</li> </ul>	no	false	true, false

### ***Hashes That Do NOT Use FIPS***

The following hash uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Hash Name	Required	Default Value	Valid Values
useHash_hmac-sha1	no	false	true, false

### ***sshUseDefaultKeyExchangeAlgorithms***

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported key exchange methods, and ignore the setting to use specific key exchange methods. When set to false, the Credential Manager only uses the selected key exchange methods.

Required	Default Value	Valid Values
no	true	true, false

### ***Key Exchange Methods That Support FIPS***

The following list of displays the Key Exchange Methods that support FIPS:

Key Exchange Method	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useKeyExchange_curve25519-sha256</li> <li>useKeyExchange_ecdh-sha2-nistp384</li> <li>useKeyExchange_ecdh-sha2-nistp256</li> <li>useKeyExchange_ecdh-sha2-nistp521</li> <li>useKeyExchange_diffie-hellman-group14-sha1</li> <li>useKeyExchange_diffie-hellman-group16-sha512</li> <li>useKeyExchange_diffie-hellman-group18-sha512</li> <li>useKeyExchange_diffie-hellman-group-exchange-sha256</li> </ul>	no	false	true, false

### ***Key Exchange Methods That Do NOT Support FIPS***

The following Key Exchange Methods use a non-FIPS method, and are ignored if you are running in FIPS mode:

Key Exchange Method	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useKeyExchange_curve25519-sha256</li> <li>useKeyExchange_diffie-hellman-group14-sha256</li> </ul>	no	true	true, false

### ***sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported server host key types, and ignore the setting to use specific ones. When set to false, the Credential Manager uses only the selected server host key types.

Required	Default Value	Valid Values
no	true	true, false

### **Host Key Types That Support FIPS**

The following list displays the Host Key Types that support FIPS:

Host Key Type	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>• useHostKeyType_ecdsa-sha2-nistp384</li> <li>• useHostKeyType_ecdsa-sha2-nistp256</li> <li>• useHostKeyType_ecdsa-sha2-nistp521</li> <li>• useHostKeyType_rsa-sha2-512</li> <li>• useHostKeyType_rsa-sha2-256</li> <li>• useHostKeyType_ssh-rsa</li> </ul>	no	false	true, false

### **Host Key Types Do NOT Support FIPS**

The following Host Key Type use a non-FIPS method, and is ignored if you are running in FIPS mode:

Host Key Type	Required	Default Value	Valid Values
useHostKeyType_ssh-ed25519	no	false	true, fals

### **Windows SSH Key Target Application External API Example**

```
POST api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "Windows SSH Key App",
  "applicationType": "windowsSshKey",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "sshKeyPairPolicyId": null,
  "attributes": {
    "extensionType": "windowsSshKey",
    "sshPort": "22",
    "sshSessionTimeout": "60000",
    "sshStrictHostKeyCheckingEnabled": "false",
    "sshKnownHostKey": "",
    "sshKnownHostKeyFingerprint": "",
    "sshUseDefaultCiphers": "true",
    "useCipher_aes128-gcm": "false",
    "useCipher_aes128-ctr": "false",
    "useCipher_aes128-cbc": "false",
    "useCipher_aes192-ctr": "false",
    "useCipher_aes192-cbc": "false",
```

```

    "useCipher_aes256-gcm": "false",
    "useCipher_aes256-ctr": "false",
    "useCipher_aes256-cbc": "false",
    "sshUseDefaultHashes": "true",
    "useHash_hmac-sha2-256": "false",
    "useHash_hmac-sha2-512": "false",
    "useHash_hmac-sha1": "false",
    "sshUseDefaultKeyExchangeAlgorithms": "true",
    "useKeyExchange_curve25519-sha256": "false",
    "useKeyExchange_ecdh-sha2-nistp384": "false",
    "useKeyExchange_ecdh-sha2-nistp256": "false",
    "useKeyExchange_ecdh-sha2-nistp521": "false",
    "useKeyExchange_diffie-hellman-group14-sha256": "false",
    "useKeyExchange_diffie-hellman-group16-sha512": "false",
    "useKeyExchange_diffie-hellman-group18-sha512": "false",
    "useKeyExchange_diffie-hellman-group-exchange-sha256": "false",
    "useKeyExchange_diffie-hellman-group14-sha1": "false",
    "sshUseDefaultServerHostKeyAlgorithms": "true",
    "useHostKeyType_ed25519": "false",
    "useHostKeyType_ecdsa-sha2-nistp384": "false",
    "useHostKeyType_ecdsa-sha2-nistp256": "false",
    "useHostKeyType_ecdsa-sha2-nistp521": "false",
    "useHostKeyType_rsa-sha2-512": "false",
    "useHostKeyType_rsa-sha2-256": "false",
    "useHostKeyType_ssh-rsa": "false"
  }
}

```

### **Windows SSH Key Target Account External API Example**

```

POST api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{
  "accountName": "keysample",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "cacheBehavior": "useCacheFirst",
  "cacheDuration": "30",
  "password": "_generate_pass_",
  "passwordViewPolicyId": "1000",
  "privileged": "t",
  "synchronize": "t",
  "useAliasNameParameter": "f",
  "attributes": {
    "extensionType": "windowsSshKey",
    "changePasswordAccount": "{other_acct_id}",
    "changeProcess": "CHANGE_PROCESS_USE_DIFFERENT_ACCOUNT_TO_CHANGE_PASSWORD"
  }
}

```

```

}
}

```

## Add a Windows SSH Password Target Connector

Use the PAM Windows SSH Password target connector to manage local account credentials on Windows systems using password-based SSH authentication.

The PAM Windows SSH Password target connector provides a secure solution for managing local privileged credentials on supported SSH-enabled Windows systems.

### NOTE

For a list of Windows versions that support the Windows SSH Password target connectors, see [Supported Platforms](#).

### TIP

The following alternative Windows connectors are available:

- **Windows SSH Key Connector:** Manages local Windows account credentials using key-based SSH authentication (most secure, also requires supported, SSH-enabled target system).
- **Windows Remote Target Connector:** Manages local Windows account credentials using the Windows Remote Desktop Service API (less secure than either SSH connector).
- **Windows Proxy Connector:** Functions similar to the Windows Remote Connector but requires the connector to be installed on a remote server in your target domain.

To add the target connector using the CLI, see [Windows SSH Password Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Windows SSH Password Target Connector External API Configuration](#).

## Add the Target Application and Connector

Follow these steps in the UI:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - **Host Name:** Select the magnifying glass to pick the target server.
  - **Device Name:** The name of the target server. Populated dynamically when you pick the target server.
  - **Application Name:** A unique application name for the specified target server.
4. In the **Application Type** field, select **Windows SSH Password**.
5. (Optional) Select a **Password Composition Policy**.  
If you do not select a password composition policy, a default policy is used. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.
6. Select the **SSH Connection** tab and complete the following fields:
  - **Port:** Enter the port that connects to the Windows host using SSH. The default value is 22.
  - **Communication Timeout:** Specify the amount of time that PAM waits for communication from the Windows host before ending the connection (in ms). The default value is 600ee00.
  - **Enable strict host key checking** (Optional) Select this option to protect against man-in-the-middle attacks by validating an SSH host key from the target server (specified in the required **Known Host Key** field) when establishing a connection.

**NOTE**

If a man-in-the-middle attack occurs, the malicious server to which your connection is redirected does not have the same SSH host key as the intended server and the connection is rejected.

- **Known Host Key** (Required if strict host key checking is enabled): Specify the base64 host key value of one of the SSH host keys configured on the target server. For example:

```
AAAAC3NzaC11ZD11NTE5AAAAIGq3L+ECE5S8CUJyZ0jiXbZReY7G/boxDUMrYlhrlK9w
```

**NOTE**

To obtain an SSH host key, you can use the [ssh-keyscan](#) utility on the target device. For example, `ssh-keyscan 127.0.0.1 2>$null` returns the IP address, host Key type and base64 host key value for all configured SSH host keys.

- **SHA256 Fingerprint** (Optional, only applicable if **Enable strict host key checking** is enabled): Specify a SHA256 fingerprint generated from the SSH host key on the target server to confirm that the value that you entered in the **Known Host Key** field matches. If the values do not match, PAM displays a dialog with an error message like the following:

```
PAM-CF-0005: Failed to validate target connector attributes. PAM-WS- 0103:Host key fingerprint does not match computed fingerprint: VpszjfaB00J5N43NQsawv1DsdeXyTzAd1bWLCak6GZl=..
```

**NOTE**

To obtain a SHA256 fingerprint, you can use the [ssh-keyscan](#) utility on the target device. For example, `ssh-keyscan 127.0.0.1 2>$null | ssh-keygen -E md5 -lf -` returns all the configured SSH host Keys and their SHA256 fingerprints.

7. Optionally, use the **Cipher**, **Hash**, **Key Exchange**, and **Server Host Key Type** tabs to configure specific encryption algorithms to use when making an SSH connection to the remote host.

**NOTE**

By default, a **Use supported...** option is set on each tab, configuring support for all available encryption algorithms, as shown in the following screenshot:

Application	SSH Connection	Cipher	Hash	Key Exchange	Server Host Key Type
Use supported ciphers: <input checked="" type="checkbox"/>					
Use aes128-gcm: <input type="checkbox"/>					
Use aes128-ctr: <input type="checkbox"/>					
Use aes128-cbc (non FIPS): <input type="checkbox"/>					
Use aes192-ctr (non FIPS): <input type="checkbox"/>					
Use aes192-cbc (non FIPS): <input type="checkbox"/>					
Use aes256-gcm: <input type="checkbox"/>					
Use aes256-ctr: <input type="checkbox"/>					
Use aes256-cbc: <input type="checkbox"/>					

**Important:** if you unset the **Use supported...** option, you *must* select at least one of the listed encryption algorithms.

- **Cipher Tab:** Unset the **Use supported ciphers** option to select specific ciphers.
- **Hash Tab:** Unset the **Use supported hashes** option to select specific hashes.
- **Key Exchange Tab:** Unset the **Use supported key exchange methods** option to select specific key exchange methods.
- **Server Host Key Type Tab:** Unset the **Use supported server host key types** option to select specific server host key types.

**NOTE**

Encryption standards continue to evolve with new vulnerabilities that are identified in what were previously accepted algorithms. Progress is also made with other more-secure cipher, hash, key exchange, or server host key options added to common utilities used for establishing secure communication channels. When upgrading PAM, be sure to consider any changes in the available more-secure cipher algorithms. Less secure ciphers, hashes, key exchanges, or server host keys algorithms are no longer listed, but continue working. However, they may be subject to removal in a future release.

8. Select **OK**.

**NOTE**

**Next Step:** [Add a Windows SSH Password target account](#).

## Windows SSH Password Target Connector CLI Configuration

This topic contains the CLI parameters for adding a Windows SSH Password target application and target account:

### Windows SSH Password Target Connector CLI Parameters

To add a Windows SSH Password target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***TargetApplication.type***

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	windowsSshPassword

#### ***Attribute.extensionType***

Required	Default Value	Valid Values
no	N/A	windowsSshPassword

#### ***Attribute.sshPort***

The TCP port used to connect to the Windows host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

#### ***Attribute.sshSessionTimeout***

When using the SSH communication channel, specifies the amount of time in milliseconds, that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

#### ***Attribute.sshStrictHostKeyCheckingEnabled***

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Strict host key checking helps to provide protection from man-in-the-middle attacks. If such an attack happens, the malicious server you are redirected to would not have the same SSH host keys as the intended server. Thus attempts to connect to such a server would fail with strict host key checking.

Required	Default Value	Valid Values
no	false	true, false

#### ***Attribute.sshKnownHostKey***

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

#### ***Attribute.sshKnownHostKeyFingerprint***

Contains the SHA-256 fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is for display purposes only. It allows the user to easily compare one key with another. The fingerprint that is specified must correspond to the specified public host key. This attribute is optional when you specify a Known Host Key. Specifying this attributes value can help you ensure that you did not make a typographical error entering the Known Host Key.

Required	Default Value	Valid Values
no	N/A	a valid public key fingerprint

#### ***Attribute.sshUseDefaultCiphers***

Specifies the default ciphers to used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported ciphers, ignoring the setting to use specific ciphers. When set to false, Credential Manager only uses the selected ciphers.

Required	Default Value	Valid Values
no	true	true, false

#### ***Ciphers That Support FIPS***



The following list displays the cipher algorithms that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useCipher_aes128-gcm</li> <li>Attribute.useCipher_aes128-ctr</li> <li>Attribute.useCipher_aes256-gcm</li> <li>Attribute.useCipher_aes256-ctr</li> <li>Attribute.useCipher_aes256-cbc</li> </ul>	no	false	true, false

### ***Ciphers That Do NOT Support FIPS***

The following list includes the algorithms that use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useCipher_aes128-cbc</li> <li>Attribute.useCipher_aes192-ctr</li> <li>Attribute.useCipher_aes192-cbc</li> </ul>	no	false	true, false

### ***Attribute.sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported hashes and ignores the setting to use specific hashes. When set to false, Credential Manager only uses the selected hashes.

Required	Default Value	Valid Values
no	true	true, false

### ***Hashes That Support FIPS***

The following list displays the hashes that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useHash_hmac-sha2-256</li> <li>Attribute.useHash_hmac-sha2-512</li> </ul>	no	false	true, false

### ***Hashes That Do NOT Use FIPS***

The following hash uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
Attribute.useHash_hmac-sha1	no	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

### ***Attribute.sshUseDefaultKeyExchangeAlgorithms***

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported key exchange methods, and ignore the

setting to use specific key exchange methods. When set to false, the Credential Manager only uses the selected key exchange methods.

Required	Default Value	Valid Values
no	true	true, false

### **Key Exchange Methods That Support FIPS**

The following list of displays the Key Exchange Methods that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useKeyExchange_curve25519-sha256</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp384</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp256</li> <li>Attribute.useKeyExchange_ecdh-sha2-nistp521</li> <li>Attribute.useKeyExchange_diffie-hellman-group14-sha1</li> <li>Attribute.useKeyExchange_diffie-hellman-group16-sha512</li> <li>Attribute.useKeyExchange_diffie-hellman-group18-sha512</li> <li>Attribute.useKeyExchange_diffie-hellman-group-exchange-sha256</li> <li>—</li> </ul>	no	false	true, false

### **Key Exchange Methods That Do NOT Support FIPS**

The following Key Exchange Methods use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useKeyExchange_curve25519-sha256</li> <li>Attribute.useKeyExchange_diffie-hellman-group14-sha256</li> </ul>	no	true	true, false

### **Attribute.sshUseDefaultServerHostKeyAlgorithms**

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported server host key types, and ignore the setting to use specific ones. When set to false, the Credential Manager uses only the selected server host key types.

Required	Default Value	Valid Values
no	true	true, false

### **Host Key Types That Support FIPS**

The following list displays the Host Key Types that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp384</li> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp256</li> <li>Attribute.useHostKeyType_ecdsa-sha2-nistp521</li> <li>Attribute.useHostKeyType_rsa-sha2-512</li> <li>Attribute.useHostKeyType_rsa-sha2-256</li> <li>Attribute.useHostKeyType_ssh-rsa</li> <li>—</li> </ul>	nofalse	false	true, false

### Host Key Types Do NOT Support FIPS

The following Host Key Type uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
Attribute.useHostKeyType_ssh-ed25519	no	false	true, false

### Windows SSH Password CLI Examples

Here is an example for adding a Windows SSH Password target application via the CLI:

```
cmdName=addTargetApplication TargetServer.hostName={host name} TargetApplication.type=windowsSshPassword
"TargetApplication.name=Windows SSH Password App" Attribute.sshPort=22
```

Here is another example for adding a Windows SSH Password target application via the CLI:

```
cmdName=addTargetAccount TargetServer.hostName= {host name} "TargetApplication.name=Windows SSH Password
App" TargetAccount.privileged=true TargetAccount.synchronize=false TargetAccount.userName=WinSshPwdAct
TargetAccount.password=sample Attribute.changeProcess=CHANGE_PROCESS_CAN_CHANGE_OWN_PASSWORD
```

## Windows SSH Password Target Connector External API Configuration

This topic describes the required and supported Attributes used when adding or updating a Windows SSH Password target application using the External API.

### Windows SSH Password Target Application External API Attributes

To add or update a Windows SSH Password target application, use the following properties as members of the `attributes` associative array included in the `body` parameter of the `/api.php/v1/devices.json/{id}/targetApplications` External API method:

#### TargetApplication.type

The target application connector type.

Required	Default Value	Valid Values
yes	N/A	windowsSshPassword

**extensionType**

Required	Default Value	Valid Values
no	N/A	windowsSshPassword

**sshPort**

The TCP port used to connect to the Windows host using SSH.

Required	Default Value	Valid Values
yes	22	0-65535

**sshSessionTimeout**

When using the SSH communication channel, specifies the amount of time in milliseconds, that Credential Manager should wait for the remote host to respond.

Required	Default Value	Valid Values
no	5000	1000-99999

**sshStrictHostKeyCheckingEnabled**

Enables or disables strict host key checking. When enabled, a connection gets established after Credential Manager compares the public key from the remote host to the public key stored in the `sshKnownHostKey` attribute. If the keys do not match, then the connection attempt is canceled.

Strict host key checking helps to provide protection from man-in-the-middle attacks. If such an attack happens, the malicious server you are redirected to would not have the same SSH host keys as the intended server. Thus attempts to connect to such a server would fail with strict host key checking.

Required	Default Value	Valid Values
no	false	true, false

**sshKnownHostKey**

Contains the base-64 encoded public host key that is associated with the target server.

Required	Default Value	Valid Values
yes if <code>sshStrictHostKeyCheckingEnabled</code> is true	N/A	a base-64 encoded SSH public host key

**sshKnownHostKeyFingerprint**

Contains the SHA-256 fingerprint of the public host key that is contained in the `sshKnownHostKey` attribute. The fingerprint is for display purposes only. It allows the user to easily compare one key with another. The fingerprint that is specified must correspond to the specified public host key. This attribute is optional when you specify a Known Host Key.

Specifying this attributes value can help you ensure that you did not make a typographical error entering the Known Host Key.

Required	Default Value	Valid Values
no	N/A	a valid public key fingerprint

### ***sshUseDefaultCiphers***

Specifies the default ciphers to used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported ciphers, ignoring the setting to use specific ciphers. When set to false, Credential Manager only uses the selected ciphers.

Required	Default Value	Valid Values
no	true	true, false

### ***Ciphers That Support FIPS***

The following list displays the cipher algorithms that support FIPS:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useCipher_aes128-gcm</li> <li>useCipher_aes128-ctr</li> <li>useCipher_aes256-gcm</li> <li>useCipher_aes256-ctr</li> <li>useCipher_aes256-cbc</li> </ul>	no	false	true, false

### ***Ciphers That Do NOT Support FIPS***

The following list includes the algorithms that use a non-FIPS method, and are ignored if you are running in FIPS mode:

Cipher Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useCipher_aes128-cbc</li> <li>useCipher_aes192-ctr</li> <li>useCipher_aes192-cbc</li> </ul>	no	false	true, false

### ***sshUseDefaultHashes***

Specifies whether the default hashes should be used when Credential Manager makes an SSH connection to the remote host.

When set to true, Credential Manager uses all supported hashes and ignores the setting to use specific hashes. When set to false, Credential Manager only uses the selected hashes.

Required	Default Value	Valid Values
no	true	true, false

### ***Hashes That Support FIPS***

The following list displays the hashes that support FIPS:

Hash Name	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useHash_hmac-sha2-256</li> <li>useHash_hmac-sha2-512</li> </ul>	no	false	true, false

### ***Hashes That Do NOT Use FIPS***

The following hash uses a non-FIPS method, and is ignored if you are running in FIPS mode:

Hash Name	Required	Default Value	Valid Values
useHash_hmac-sha1	no	hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96	A comma-separated list containing one or more of the following values: hmac-md5,hmac-sha1, hmac-sha1-96, hmac-md5-96. Do not use spaces in the list.

### ***sshUseDefaultKeyExchangeAlgorithms***

Specifies whether the default key exchange methods are used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported key exchange methods, and ignore the setting to use specific key exchange methods. When set to false, the Credential Manager only uses the selected key exchange methods.

Required	Default Value	Valid Values
no	true	true, false

### ***Key Exchange Methods That Support FIPS***

The following list of displays the Key Exchange Methods that support FIPS:

Key Exchange Method	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useKeyExchange_curve25519-sha256</li> <li>useKeyExchange_ecdh-sha2-nistp384</li> <li>useKeyExchange_ecdh-sha2-nistp256</li> <li>useKeyExchange_ecdh-sha2-nistp521</li> <li>useKeyExchange_diffie-hellman-group14-sha1</li> <li>useKeyExchange_diffie-hellman-group16-sha512</li> <li>useKeyExchange_diffie-hellman-group18-sha512</li> <li>useKeyExchange_diffie-hellman-group-exchange-sha256</li> </ul>	no	false	true, false

### ***Key Exchange Methods That Do NOT Support FIPS***

The following Key Exchange Methods use a non-FIPS method, and are ignored if you are running in FIPS mode:

Key Exchange Method	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useKeyExchange_curve25519-sha256</li> <li>useKeyExchange_diffie-hellman-group14-sha256</li> </ul>	no	true	true, false

### ***sshUseDefaultServerHostKeyAlgorithms***

Specifies whether the default host key types should be accepted used when Credential Manager makes an SSH connection to the remote host. When set to true, the Credential Manager uses all supported server host key types, and ignore the setting to use specific ones. When set to false, the Credential Manager uses only the selected server host key types.

Required	Default Value	Valid Values
no	true	true, false

### ***Host Key Types That Support FIPS***

The following list displays the Host Key Types that support FIPS:

Host Key Type	Required	Default Value	Valid Values
<ul style="list-style-type: none"> <li>useHostKeyType_ecdsa-sha2-nistp384</li> <li>useHostKeyType_ecdsa-sha2-nistp256</li> <li>useHostKeyType_ecdsa-sha2-nistp521</li> <li>useHostKeyType_rsa-sha2-512</li> <li>useHostKeyType_rsa-sha2-256</li> <li>useHostKeyType_ssh-rsa</li> <li>—</li> </ul>	nofalse	false	true, false

### ***Host Key Types Do NOT Support FIPS***

The following Host Key Type use a non-FIPS method, and is ignored if you are running in FIPS mode:

Host Key Type	Required	Default Value	Valid Values
useHostKeyType_ssh-ed25519	no	false	true, fals

### **Windows Target Application External API Example**

Here is an example for adding a Windows SSH Password target application via the External API:

```
POST api.php/v1/devices.json/{deviceId}/targetApplications
{
  "applicationName": "Windows SSH Password App",
  "applicationType": "windowsSshPassword",
  "description1": "sample descriptor1",
  "description2": "sample descriptor2",
  "passwordCompositionPolicyId": null,
  "attributes": {
    "extensionType": "windowsSshPassword",
```

```

    "sshPort": "22",
    "sshSessionTimeout": "60000",
    "sshStrictHostKeyCheckingEnabled": "false",
    "sshKnownHostKey": "",
    "sshKnownHostKeyFingerprint": "",
    "sshUseDefaultCiphers": "true",
    "useCipher_aes128-gcm": "false",
    "useCipher_aes128-ctr": "false",
    "useCipher_aes128-cbc": "false",
    "useCipher_aes192-ctr": "false",
    "useCipher_aes192-cbc": "false",
    "useCipher_aes256-gcm": "false",
    "useCipher_aes256-ctr": "false",
    "useCipher_aes256-cbc": "false",
    "sshUseDefaultHashes": "true",
    "useHash_hmac-sha2-256": "false",
    "useHash_hmac-sha2-512": "false",
    "useHash_hmac-sha1": "false",
    "sshUseDefaultKeyExchangeAlgorithms": "true",
    "useKeyExchange_curve25519-sha256": "false",
    "useKeyExchange_ecdh-sha2-nistp384": "false",
    "useKeyExchange_ecdh-sha2-nistp256": "false",
    "useKeyExchange_ecdh-sha2-nistp521": "false",
    "useKeyExchange_diffie-hellman-group14-sha256": "false",
    "useKeyExchange_diffie-hellman-group16-sha512": "false",
    "useKeyExchange_diffie-hellman-group18-sha512": "false",
    "useKeyExchange_diffie-hellman-group-exchange-sha256": "false",
    "useKeyExchange_diffie-hellman-group14-sha1": "false",
    "sshUseDefaultServerHostKeyAlgorithms": "true",
    "useHostKeyType_ed25519": "false",
    "useHostKeyType_ecdsa-sha2-nistp384": "false",
    "useHostKeyType_ecdsa-sha2-nistp256": "false",
    "useHostKeyType_ecdsa-sha2-nistp521": "false",
    "useHostKeyType_rsa-sha2-512": "false",
    "useHostKeyType_rsa-sha2-256": "false",
    "useHostKeyType_ssh-rsa": "false"
  }
}

```

### **Windows Target Account External API Example**

Here is another example for adding a Windows SSH Password target application via the External API:

```

POST api.php/v1/devices.json/{deviceId}/targetApplications/{applicationId}/
targetAccounts
{

```



```

"accountName": "WinSshPwdApp",
"description1": "sample descriptor1",
"description2": "sample descriptor2",
"cacheBehavior": "useCacheFirst",
"cacheDuration": "30",
"password": "sample",
"passwordViewPolicyId": "1000",
"privileged": "t",
"synchronize": "f",
"useAliasNameParameter": "f",
"attributes": {
  "extensionType": "windowsSshPassword",
  "changeProcess": "CHANGE_PROCESS_CAN_CHANGE_OWN_PASSWORD"
}
}

```

## Add a Windows Remote Target Connector

The Windows Remote target connector lets PAM manage Windows accounts and the passwords for services and scheduled tasks that are local to the Windows server. The Windows Remote Target Connector is an alternative to the Windows Proxy Connector, but does not require that you install software in the Windows domain.

### NOTE

Starting in PAM 4.1.5, the Windows Remote connector does not support target accounts that are members of the [Windows Protected Users Security Group](#) and [Add a Windows Remote Target Connector](#).

### TIP

The following alternative Windows connectors are available:

- **Windows SSH Key Connector:** Manages local Windows account credentials using key-based SSH authentication (most secure, but requires supported, SSH-enabled target system).
- **Windows SSH Password Connector:** Manages local Windows account credentials using password-based SSH authentication (most secure, but requires supported, SSH-enabled target system).
- **Windows Proxy Connector:** Functions similar to this Windows Remote Connector but you must install the connector on a remote server in your target domain. See [Add a Windows Proxy Connector](#).

This connector uses Samba commands and remote Windows API calls to make updates to the account, services, and scheduled tasks passwords. To complete discovery and password changes for services and scheduled tasks, the connector might incur extra overhead.

To add the target connector using the CLI, see the [Windows Remote Target Connector CLI Configuration](#).

To add the target connector using the external API, see [Windows Remote Target Connector External API Configuration](#).

### Prerequisites for Using the Windows Remote Connector

Complete the following prerequisite steps to prepare your environment to support the Windows Remote Connector:

1. To configure Windows Remote target accounts, first [create a device](#) (target server) that is assigned a device type of Password Management.

**NOTE**

Use the private IP address of an AWS or Azure Windows device. Some features do not function properly when you use the public IP address.

2. Prepare the target server for using the Windows Remote Connector with the following information:
    - **Ports Used by the Connector**  
The Windows Remote Connector requires these ports to be open in the firewall:
      - SMB: port 445
      - WMI: port 135 and port range from 49152 through 65535 or 1024 through 4999
    - **Disable the Guest Account**  
If the guest account in the domain or on the target server is enabled, the connector tries to verify its password, which does not exist. Disable this account to prevent a false password verification
    - **User Access Control workaround**  
If User Access Control is enabled on the target server and the account for password management is a local administrator, the connector needs access to perform SMB and WMI operations. To give the connector access, add the LocalAccountTokenFilterPolicy registry setting to remove remote restrictions:
 

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
\LocalAccountTokenFilterPolicy = dword:00000001
```
- NOTE**  
WMI traffic is encrypted. When a password is updated through WMI, the password is encrypted.
- **Review Group or Local Policy Security Options**  
The default values for network security on Windows systems allow the Windows Remote Connector to function. However, if certain settings are set too restrictive, Windows Remote password management fails. To ensure that Windows Remote operates effectively, verify the following settings in the Group or Local Policy Security Options. Go to Start, Administrative Tools, Local Security Policy, Local Policies, Security Options.
    - **Network security: Restrict NTLM: Incoming NTLM traffic**  
Allow all, or Not Defined
    - **Network security: Restrict NTLM: NTLM authentication in this domain**  
Disable, Not Defined, or Deny for domain accounts
  - **Set the Local System Context**  
The Windows Remote Connector can be run in the context of a local system. This scenario allows successful management and updates of the local Windows accounts, service passwords, and scheduled task passwords. The Windows Remote Administrator account that you add to the appliance must be part of the Local Administrator group on the target server.
3. To use a Windows Domain account

**Add the Target Application and Connector****Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Fill in the following fields:
  - **Host Name:** The hostname of the target server.
  - **Device Name:** The name of the target device.
  - **Application Name:** The name must be unique.
4. In the **Application Type** field, select **Windows Remote**.
5. (Optional) Select a password composition policy.

**NOTE**

If you do not select a password composition policy, a default policy is used. This policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.

6. If you are using target groupings, add Descriptors.
7. Select the **Windows Remote** tab.
8. For the **Account Type**, select one of the following options:
  - **Local Account:** Manage local accounts on target servers.
  - **Domain Account:** Manage Windows Domain accounts. We recommend using the [Active Directory connector](#) to manage Domain Accounts.

If you set the **Domain Account** option, select one of the following options from the drop-down list that becomes active:

  - **Target Server is Domain Controller:** (For domain administrator accounts only) Use the target server as the domain controller.
  - **Domain Controllers are on servers:** Specify the IP address or addresses (comma-separated) of domain controllers in the **Specify Servers** text field. If there are multiple entries, PAM uses the first reachable domain controller. Enter one or more servers, which are separated by commas.

**NOTE**

To support Kerberos authentication (see **Use Kerberos** later in this topic), you must specify the FQDNs of domain controllers instead of IP addresses.

- **Lookup Domain Controllers in DNS:** Use the first reachable DNS server that is configured in the [PAM server network settings](#) to look up the domain controller.
  - **Lookup Domain Controllers in specified:** Specify the IP address or (comma-separated) addresses of one or more DNS servers to use to look up the domain controller in the **Specify DNS** text field. If there are multiple entries, PAM uses the first reachable DNS server in the list to look up the domain controller.
  - **Use Kerberos:** (Optional) Set this option to enable authentication using the Kerberos protocol. The name of the Kerberos realm is displayed in the **Realm Name** field that appears below the **Domain Name** field lower on the dialog.
- Kerberos verifies user identities using a Key Distribution Center (KDC), which is a service that runs on Windows domain controllers. PAM uses the KDC on the domain controller which is determined by the previously configured **Domain Account** setting.

**NOTE**

If an existing Windows Remote target application has the same domain name but a different Domain Controller lookup option than the one specified in this definition, a popup appears stating that you should use the Domain Controller lookup option. However, you can override this suggestion and keep the Domain Controller lookup specified here.

- Complete the following fields in the **DNS Servers** section:
    - **Domain Name:** Specify the Windows domain of the managed account.
    - **Active Directory Site:** (Optional) Specify an Active Directory directory site name to narrow the search for domain controllers. If the field is empty, PAM searches for all domain controllers who are identified by the DNS server. (This field is Inactive if the "Target Server is Domain Controller" **Domain Account** option is specified.)
    - **DC replication time (in ms):** Enter the frequency of replication in milliseconds.
  - **Active Directory Connect Timeout:** Enter the timeout for connecting to AD, in milliseconds.
  - For **Active Directory Read Timeout:** Enter the timeout for reading from AD, in milliseconds.
9. If you enabled [Account Discovery](#), complete the following settings on the **Account Discovery** tab:

**NOTE**

**Account Discovery** is only supported for **Local Accounts**.

- **Account Filter:** (Optional) Specify a filter to limit the accounts that are discovered from the Windows server.

**NOTE**

The only valid wildcard character in filters is an asterisk (\*).

- **Discover Services:** Set this option to also discover services.
- **Discover Tasks:** Set this option to also discover tasks.

10. Select **OK** to save the application.

**NOTE**

Next step: [Configure Windows Remote Target Accounts](#).

**Windows Remote Target Connector CLI Configuration**

This topic contains the parameters for adding a Windows Remote target application and target account:

**Windows Remote Target Connector CLI Parameters**

To add a Windows Remote target application and connector using the CLI, use the `addTargetApplication` command and the following command parameters:

***Attribute.extensionType***

Specify the type of account to use.

Required	Default Value	Valid Values
yes	N/A	windowsRemoteAgent

***Attribute.accountType***

The type of account being managed.

Required	Default Value	Valid Values
yes	domain	domain, local

***Attribute.domainName***

The Windows domain for the managed accounts.

Required	Default Value	Valid Values
Required if <code>Attribute.accountType</code> is set to domain (the default).	none	Domain name (a text string)

***Attribute.domain***

The Windows domain for the managed accounts. This attribute exists only for backwards compatibility. We recommend using `Attribute.domainName` instead.

Required	Default Value	Valid Values
Required if <code>Attribute.accountType</code> is set to domain (the default).	none	Domain name (a text string)

***Attribute.useDNS***

Determine the level to which DNS is used.

Required	Default Value	Valid Values
Required if <code>Attribute.accountType</code> is set to domain (the default).	none	<ul style="list-style-type: none"> <li><code>noDNS</code> : DNS is not used</li> <li><code>retrieveDNS</code> : Retrieve the DNS server that the Credential Manager server uses</li> <li><code>specifiedDNS</code> : Use the DNS server that is specified by the <code>dnsServer</code> attribute</li> </ul>

### ***Attribute.dnsServer***

The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if <code>Attribute.useDNS</code> is set to <code>specifiedDNS</code> .	none	Comma separated list of DNS server host names.

### ***Attribute.specifiedServersList***

Provide a comma separated list of domain controllers.

Required	Default Value	Valid Values
Required if <code>Attribute.useDNS</code> is set to <code>specifiedServers</code> .	none	Comma separated list of valid domain controllers

### ***Attribute.adSite***

The Active Directory site. This parameter is only used if `Attribute.useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers, using the specified name.

Required	Default Value	Valid Values
no	none	String

### ***Attribute.enableKerberos***

Determines whether Kerberos authentication is enabled for a target application.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li><code>true</code> - Kerberos authentication is enabled.</li> <li><code>false</code> - Kerberos authentication is not enabled.</li> </ul>

### ***Attribute.overrideDnsType***

If Kerberos is enabled, specifies whether to allow a different DNS lookup type for this target application than for others in the same domain.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>true - a different DNS lookup type is allowed for this target application.</li> <li>false - a different DNS lookup type is not allowed for this target application.</li> </ul>

### Windows Remote Target Account CLI Parameters

To add a Windows Remote target account that uses the target connector, use the `addTargetAccount` command and the following parameters:

#### ***Attribute.extensionType***

Specify the extension type to use.

Required	Default Value	Valid Values
yes	N/A	windowsRemoteAgent

#### ***Attribute.accountType***

Specify the type of account to use.

Required	Default Value	Valid Values
yes	user	user, admin

#### ***Attribute.useOtherAccountToChangePassword***

Specify whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false

#### ***Attribute.otherAccount***

Specify which other account to use to perform password change requests.

Required	Default Value	Valid Values
Required if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	A valid target account ID.

**Note:** The Target Account ID can be found using the `searchTargetAccount` command.

#### ***Attribute.serviceInfo***

List of services.

Required	Default Value	Valid Values
no	N/A	Add the following code for each service: <code>hostname: servicename:restart</code> <code>hostname: servicename:norestart</code> <code>hostname</code> is the server hosting the service Delimit multiple services with the   (pipe) character. An empty string means no services.

### ***Attribute.tasks***

List of scheduled tasks.

Required	Default Value	Valid Values
no	none	For each task, add the string: <code>hostname: taskname</code> Delimit multiple services with the   (pipe) character. <code>hostname</code> is the name of the server where the scheduled task is hosted An empty string means no tasks.

### ***Attribute.forcePasswordChange***

This parameter specifies whether Credential Manager updates passwords that fail verification during an initial synchronization. The default value is false. To update passwords that fail initial synchronization, set the attribute value to true.

Required	Default Value	Valid Values
no	false	true, false

### **Windows Remote CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myWindowsRemote TargetApplication.type=windowsRemoteAgent
Attribute.extensionType=windowsRemoteAgent Attribute.accountType=domain Attribute.domainName=testDomain
Attribute.enableKerberos=true

cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com TargetApplication.name=myWindowsRemote
TargetAccount.userName=admin TargetAccount.password=P@ssw0rd TargetAccount.privileged=true
Attribute.extensionType=windowsRemoteAgent Attribute.accountType=admin
Attribute.useOtherAccountToChangePassword=false Attribute.forcePasswordChange=false
Attribute.serviceInfo=HostA:servicename:restart|HostB:ServiceName:norestart Attribute.tasks=HostA:taskName|
HostB:taskName
```

## **Windows Remote Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating Windows Remote target applications using the External API.

## Windows Remote Target Application External API Attributes

To add or update a Windows Remote target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call.

### ***accountType***

The type of account being managed.

Required	Default Value	Valid Values
yes	domain	domain, local

### ***domainName***

The Windows domain for the managed accounts.

Required	Default Value	Valid Values
Required if <code>accountType</code> is set to domain (the default).	none	Domain name (a text string)

### ***domain***

The Windows domain for the managed accounts. This attribute exists only for backwards compatibility. We recommend using `domainName` instead.

Required	Default Value	Valid Values
Required if <code>accountType</code> is set to domain (the default).	none	Domain name (a text string)

### ***useDNS***

Determine the level to which DNS is used.

Required	Default Value	Valid Values
Required if <code>accountType</code> is set to domain (the default).	none	<ul style="list-style-type: none"> <li><code>noDNS</code> : DNS is not used</li> <li><code>retrieveDNS</code> : Retrieve the DNS server that the Credential Manager server uses</li> <li><code>specifiedDNS</code> : Use the DNS server that is specified by the <code>dnsServer</code> attribute</li> </ul>

### ***dnsServer***

The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if <code>useDNS</code> is set to <code>specifiedDNS</code> .	none	Comma separated list of DNS server host names.

### ***specifiedServersList***



Provide a comma separated list of domain controllers.

Required	Default Value	Valid Values
Required if <code>useDNS</code> is set to <code>specifiedServers</code> .	none	Comma separated list of valid domain controllers

### ***adSite***

The Active Directory site. This parameter is only used if `useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers, using the specified name.

Required	Default Value	Valid Values
no	none	String

### ***enableKerberos***

Determines whether Kerberos authentication is enabled for a target application.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>t - Kerberos authentication is enabled.</li> <li>f - Kerberos authentication is not enabled.</li> </ul>

### ***overrideDnsType***

Determines whether a Kerberos-enabled application supports a different domain controller lookup type than an existing Kerberos-enabled Windows Remote target application in the same domain.

Required	Default Value	Valid Values
no	false	<ul style="list-style-type: none"> <li>t - A different domain controller lookup type is supported.</li> <li>f - A different domain controller lookup type is not supported.</li> </ul>

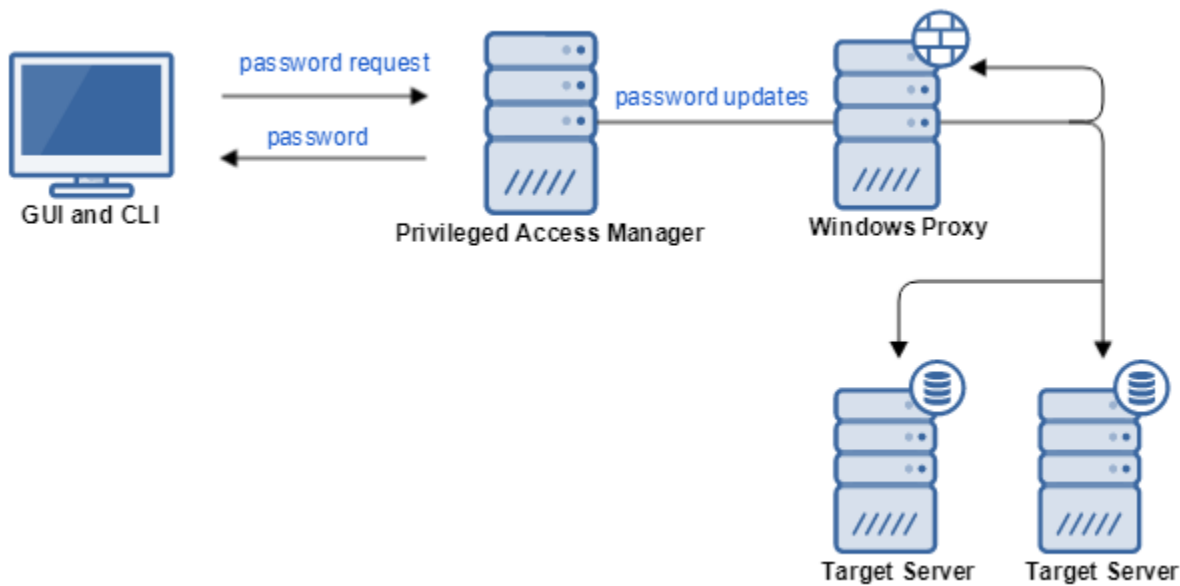
### **Windows Remote External API Example**

```
{
  "applicationName": "myWindowsRemote",
  "applicationType": "windowsRemoteAgent",
  "attributes": {
    "accountType": "domain",
    "domainName": "testDomain",
  }
}
```

## **Add a Windows Proxy Connector**

The Windows Proxy connector manages Windows accounts. To use the Windows Proxy connector, you must install the connector on a remote server in your target domain.

The following graphic shows where the Windows Proxy resides in your environment.

**Figure 25: Windows Proxy architecture****TIP**

Two other Windows connectors are available:

- Windows Remote Target Connector - functions similar to the Windows Proxy but it does not require you to install any component in your target domain. See [Windows Remote Target Connector](#).
- Active Directory Connector - manages passwords of Active Directory accounts. See [Active Directory Target Connector](#).

Use the Windows Proxy connector to manage passwords for:

- Active Directory accounts
- Local Windows accounts
- Windows services
- Windows scheduled tasks

The Windows Proxy Connector uses Windows APIs to make updates to these passwords. The connector queries one or more DNS servers to find domain controllers. The Windows Proxy connector uses HTTPS and AES encryption for secure communications.

The permissions that are required for the Windows Proxy are affected by several architectural deployment decisions:

- The type of accounts being managed by the proxy: local, domain, or both.

**NOTE**

**Account Discovery** is only supported for **Local Accounts**.

- Whether passwords on services and scheduled tasks are also being managed
- Whether the proxy is deployed on each server, or whether one proxy is deployed for the domain.

To manage only local accounts, you deploy the proxy on each managed server and run the proxy in the "local system" context. This scenario allows successful updates to the local accounts, services, and scheduled tasks.

If you deploy a proxy to manage multiple servers, it must operate under an account with privileges to manage the accounts, services, and scheduled tasks. If you use the Active Directory connector to manage the domain accounts, then the proxy must run with a domain account that has those privileges.

As a result, the service account that is used for the proxy can limit its privileges to a Domain User. To enable "local system" management, the service account must be a member of the Local Administrator group on the managed Target Account server.

To use the Windows Proxy to manage Domain accounts, add the service account to the domain Account Operators group. The proxy can then reset passwords in Active Directory.

### **Next Steps**

- [How to Install a Windows Proxy for Credential Manager](#)
- [Add Windows Proxy Target Applications and Accounts](#)
- [Windows Proxy Target Connector CLI Configuration](#)
- [View Windows Proxy Logs](#)

## **How to Install a Windows Proxy for Credential Manager**

The Windows Proxy is a software component of Privileged Access Manager Credential Manager. Install it to enable updating Windows-based account passwords, and updating Windows service and scheduled task login account passwords. For basic information about the Windows Proxy, see [Add a Windows Proxy Connector](#).

The sections in this topic describe how to install a Windows Proxy.

### **About Windows Accounts**

The following table describes the various Windows user accounts. Windows service accounts allow system administrators to control the permission level that is granted to a Windows service. Windows services that access network resources might require a restart when the associated user account password is changed.

Windows account types	Who can change the password?	Description
Local user	Local user Local administrator account	An account with local system privileges on a Windows system that a user accesses.
Domain user	Domain user Domain administrator	A network-based user account. Domain user accounts provide users with access to network resources. A domain user account is authenticated against Active Directory.
Local administrator	Local administrator	A local administrator account has administrator privileges on the local system, but does not have Network Administrator privileges. A local administrator cannot change domain user account passwords.
Domain administrator	Domain administrator	A domain administrator account has administrator privileges throughout the domain. A domain administrator requires local administrator privileges to update local accounts.  By default, when a system joins the domain, the domain administrator is given local administrator access.

### **Windows Proxy Configuration**

The configuration of the Windows Proxy depends on the type of accounts you are managing and whether your network is part of a domain.

You can install as many Windows Proxies as you need. You must install a minimum of one Windows Proxy for each domain or workgroup. The Windows Proxy service must run as a domain administrator or local administrator. By default, the Windows Proxy installs with local service permissions. You must update the local service permissions to manage passwords over a network connection.

The following table lists the target host and target account registration notes associated with the various Windows Proxy installation options.

Windows Proxy service runs as:	Target user account type	Target host configuration notes	Target Account Registration notes
Domain administrator	Domain	The domain administrator must have local administrator privileges on the target host.	When adding the target account, select the option Use Proxy credentials to change password.
Domain administrator	Local (target host)	The account being managed (on the target host) must have Log in local user rights.	When adding the target account, the account that is selected to manage passwords must have Local Administrator privileges.
Local administrator (Proxy host)	Domain	Not recommended	Not recommended
Local administrator (Proxy host)	Local (target host)	None	When adding the target account, the account that is selected to manage passwords must have local administrator privileges.

## WARNING

If Privileged Access Manager manages the administrator account that the Windows Proxy service runs as, do *not* configure this account to change its own password. The Windows service cannot restart itself after a password change. Instead, use a second Windows Proxy running as a different account to manage the service account. Use a separate target application that only uses the remote proxy. When you configure the Windows target account for the Windows Proxy, discover the proxy service and set the **Start/Restart** option. This option allows Privileged Access Manager to restart the service on a password change.

The accounts that are associated with the two Windows Proxy services must be in the Administrators group on their proxy hosts. The proxies can then manage other accounts on either host, or on remote hosts with target applications that have selected both proxies for high availability.

When verifying the passwords of Windows Proxy target applications, Credential Manager connects to target servers using the Windows Proxy.

When adding a domain controller target server, use the domain controller NetBIOS name as the target server host name.

You can register the Windows Proxies in Credential Manager manually or automatically. Upon receipt of the Windows Proxy login, the server automatically adds the Windows Proxy in an inactive state and flags the request in the UI.

A Windows Proxy is not configured as a managed object device, so the proxy does not appear in the Device list. However, this same host can still be the target of a Privileged Access Manager managed object. The same host can be used for access or password management as a device.

When the Privileged Access Manager server sends sensitive information to a Windows Proxy, that information is encrypted using the Windows Proxy key. The key is unique for each Windows Proxy. The UI provides a button to update the Windows Proxy key.

## **Windows Proxy Requirements**

This section details the hardware and software requirements for the Windows Proxy.

### ***Hardware Requirements***

The Windows Proxy requires 128 MB of RAM and 180 MB of hard drive space. The Windows Proxy log file requires 50 MB.

### ***Operating System Requirements***

For a list of Windows operating system versions that support the Windows Proxy, see [Supported Environments](#).

## **Prepare for Windows Proxy Installation**

Complete the following tasks to prepare to install the Windows Proxy:

- Verify that firewalls do not block necessary communication ports. See [Default Ports for Credential Manager](#).
- Verify that DNS resolution of the Windows Proxy host succeeds on the Privileged Access Manager server. If DNS resolution of the server fails on the Windows Proxy host, the Windows Proxy hosts file (C:\Windows\System32\drivers\etc\hosts) requires an entry for the server.
- Verify that DNS resolution of the Privileged Access Manager server succeeds on the Windows Proxy host.
- Disable Windows Simple File Sharing on all Windows servers that have accounts being managed through the Windows Proxy.  
Follow these steps:
  - a. Select **Start**.
  - b. Select **My Computer**.
  - c. Select **Organize** or **View**, depending upon your Windows version.
  - d. Select **Options** and **Folder and Search Options**, depending upon your Windows version.
  - e. Select the **View** tab.
  - f. At the bottom of **Advanced Settings**, disable **Use Sharing Wizard (Recommended)**.  
If you enable the sharing wizard, the Windows Proxy cannot synchronize and update accounts, and the Windows Proxy error log returns a 1326-ERROR\_LOGON\_FAILURE message.
- If the Guest account in the domain or on the target server is enabled, the Windows Proxy Connector appears to verify the password. However, that target account password does not exist on the target server. Disable the guest account in the domain or on the target server to avoid this false password verification.

You can install the Windows Proxy and an A2A Client on the same Windows host. Do not use the same installation folder for both the Windows Proxy and the A2A Client. The installation of either component overwrites the Credential Manager component that is already installed in that folder.

The default values for Network Security on Windows systems allow Windows Proxy to function. If certain settings are set too restrictively, the Windows Proxy can fail. Verify these settings in the Group or Local Policy Security Options:

- **Network security: Restrict NTLM: Incoming NTLM traffic**  
Allow all, or Not Defined
- **Network security: Restrict NTLM: NTLM authentication in this domain**  
Disable, Not Defined, or Deny for domain accounts

## **Download the Windows Proxy Software**

Download the Windows Proxy software (WindowsProxy-X.x(x).zip) from the Broadcom Support site. For information on how to download the software, see [Download PAM Installation Media](#).

## **Install the Windows Proxy Software**

The wizard installs the Windows Proxy software.

### **NOTE**

Installing more than one Windows Proxy on the same host is not supported. Installing into the same directory overwrites the Windows Proxy already installed in that directory. Always uninstall an existing Windows Proxy before installing a newer version.

### **NOTE**

The wizard fails when you execute it from an account that contains special characters. To avoid this error, start the installation by right-clicking on the executable file and selecting the **Run As** option. The **Run As** dialog opens and prompts for an alternate username and password to use for the installation. Specify the account credentials and continue with the installation.

### **Follow these steps:**

1. Navigate to the location where you unzipped the installation package.
2. Start the `setup_windows_agent.exe` installation wizard.
3. In the Introduction window, select **Next**.
4. In **Choose Install Folder** window, enter, or select the folder where you want to install the proxy, and select **Next**. We recommend that you do not use a space character in the root folder, the name of the installation location, or the folder name.
5. In the **Server Information** window, enter the Fully Qualified Domain Name (FQDN) of the Privileged Access Manager server in the **Server Name** field. If you want the Windows Proxy Agent to communicate to the PAM appliance using an IPv6 address, select **IPv6 Enabled**.

### **NOTE**

If the **IPv6 Enabled** option is set, verify that both the Agent and PAM are configured with IPv6 addresses.

6. Select **Next** to confirm your choices and display the **Pre-Installation Summary** window.
7. In the **Pre-Installation Summary** window, validate the installation information then select **Install**.
8. When the installation finishes and the Install Complete window appears, select **Done**.

## **Start the Windows Proxy Service**

To start the Windows service (`PAM Proxy`) on a Windows server, complete *one* of the following procedures:

- Open a command window and enter the following text: `net start "PAM Proxy"`
- Start the **PAM Proxy** service using the Services Administrative tool:  
The steps to start the service using the Windows Services Administrative tool depend on your Windows platform. For example, to start the service with Windows 7, select Start, Control Panel, Administrative Tools, Services. Then select **PAM Proxy** in the Services list and then select **Start**.

## **Activate the Windows Proxy**

After the Windows service is running on the Windows server, active the Windows Proxy from the PAM UI.

### **Follow these steps:**

1. From the UI, go to Credentials, Manage Targets, Proxies.
2. Select the new proxy entry and select **Update**.
3. Select the **Active** checkbox then select OK.

## **Stop the Windows Proxy**

Do *one* of the following steps:

- Stop the **PAM Proxy** service using the Services Administrative tool.  
Stopping the service using the Windows Services Administrative tool depends on your Windows platform. For example, to stop the service with Windows 7, select Start, Control Panel, Administrative Tools, Services, select **PAM Proxy** in the Services list, and then select Stop.
- Open a command line window and type the following command: `net stop "PAM Proxy"`

### Related Topics

- [Add Multiple Windows Proxies](#)
- [Configure a Windows Proxy to Use a Windows Domain Account](#)
- [Modify the Windows Proxy Configuration File](#)
- [Uninstall a Windows Proxy](#)

## Add Multiple Windows Proxies

You add multiple proxies in Privileged Access Manager to support managing multiple domains, improve load balancing and redundancy of your network.

For general information about Windows Proxies, see [Configure a Windows Proxy Connector](#).

### WARNING

Install the Windows Proxy software on a Windows host before adding a proxy to Credential Manager. See [Install a Windows Proxy for Credential Manager](#). The Windows Proxy runs as service on the Windows host. During the installation process:

1. Identify the Privileged Access Manager appliance with which the proxy registers.
2. Access the proxy list by selecting Targets, Proxies.
3. Activate the proxy by opening the proxy record in that list and changing its Status to "Active".

Use the following procedure to add a proxy manually and register it automatically.

### Follow these steps:

1. Select **Credentials, Manage Targets, Proxies**. The Proxy List page appears.
2. Select **Add**.  
The Proxy Details page appears.
3. In the **Host Name** field, enter the DNS host name or IP address where the proxy software resides.
4. In the **Device Name** field, assign a name to the Device.
5. In the **IP Address** field, enter the IP address of the host.
6. To activate the proxy, select the **Active** checkbox. Otherwise, clear the box.
7. To prevent the host name from being overwritten each time the client registers, set the **Preserve Host Name** option. Otherwise, clear the option.  
The default option for this setting is determined on the **Settings, Credential Manager** page. See the **Preserve Client/Proxy Host Names** checkbox on the **Request Server Settings** tab.
8. If you are using target groupings, enter the proxy descriptor information in the **Descriptor** fields.
9. Select **OK** to save.

## Configure a Windows Proxy to Use a Windows Domain Account

You might want the Windows Proxy to use a Windows Domain account to provide the privileges necessary to manage Windows Proxy Target Accounts. You must have local administrator privileges to change the Windows Proxy settings.

**Follow these steps on the device that hosts the Windows Proxy:**

1. Select **Start, Control Panel, Administrative Tools, Services**.
2. Right click on **PAM Proxy** and select **Properties**.
3. Select on the **Log On** tab.
4. Select **This Account** radio button.
5. Enter the Domain and Windows account names for the account. For example: NT-01\joedoe or joedoe@ca.com

**Modify the Windows Proxy Configuration File**

You can modify the Windows Proxy configuration file to address certain scenarios, such as:

- Changing a configuration that is not included in the installer, for example, port numbers.
- Applying a configuration change after installation such as changing the log file location.
- Modifying the logging level to debug a problem.

The Windows Proxy configuration file is located here:

```
C:\<install_home>\cloakware\cspmclient\config\cspm_client_config.xml
```

Where `<install_home>` is the location and name of your installation folder, for example Program Files \cspm\_agent.

The following table describes the XML tags in the Windows Proxy configuration file.

XML Tag	Description
<code>&lt;applicationtype&gt;</code>	Valid value is <code>cspm_agent</code> . If this value is set to <code>cspm_agent</code> , the Credential Manager client starts with Windows Proxy functionality. <code>cspm_agent</code> is supported only on Windows platforms.
<code>&lt;cacheallow&gt;</code>	Enables or disables caching for the Credential Manager client. The default value is <code>true</code> .
<code>&lt;loglevel&gt;</code>	Specifies the log level. Valid values are <code>severe</code> , <code>warning</code> , <code>info</code> , <code>fine</code> and <code>off</code> . Entry is case insensitive. The default value is <code>warning</code> . The <code>off</code> setting means log messages are not generated.
<code>&lt;cspmserver&gt;</code>	Specifies the host name of the Privileged Access Manager appliance. This value is set by the installer.
<code>&lt;cspmserver_port&gt;</code>	The default port on which the Privileged Access Manager appliance listens. The default is blank. For HTTPS, the default is 443. If the server port is changed from 443, you must modify this value
<code>&lt;daemonserver1_port&gt;</code>	The Windows Proxy uses this port to listen for requests from the Privileged Access Manager appliance. For the Windows Proxy, the default value is 27077.
<code>&lt;daemonserver2_port&gt;</code>	This port is not used by the Windows Proxy.
<code>&lt;logfile&gt;</code>	Specifies the location of the log file that is used by the daemon. The installer sets this value.



<c_logfile>	The log file that is used by the service and stateless client interface stubs. The default is: C:\WINDOWS\TEMP\cspm_c_client_log.txt on Windows Server 2008 R2. The log file must be in a directory to which all users of the Windows Proxy have write access.
<operation>	For internal use only.

## Uninstall a Windows Proxy

You can uninstall a Windows Proxy from a Windows client when it is no longer needed.

### Follow these steps:

1. Stop the Windows Proxy using one of the following steps:
  - Stop the **PAM Proxy** service using the Windows Services tool.
  - Open a Command Prompt window and enter the following command:  
net stop "PAM Proxy"
2. Use one of the following methods to launch the uninstall executable:
  - Use the Control Panel Add/Remove Programs option: Select the **Windows Proxy** entry
  - Navigate to C:\cspm\_agent\Cloakware\cspmclient\Uninstall\_Password\_Authority\_Windows\_Proxy and double-click Uninstall PAM Proxy.exe .
  - Open a Command Prompt window and run the uninstall script:  
C:\cspm\_agent\Cloakware\cspmclient\Uninstall\_Password\_Authority\_Windows\_Proxy  
\"Uninstall PAM Proxy.exe"

Ensure that you enclose the file name within double quotes.  
The greeting window appears followed by the **Uninstall Windows Proxy** window.
3. Select **Uninstall**.  
The **Uninstall Windows Proxy** status window appears.  
When the uninstall finishes, the **Uninstall Complete** window appears. You might need to remove files manually. If so, the uninstaller identifies the files that must be manually removed.
4. Select **Done**.
5. (Optional) Remove the empty cspm\_agent folder.

## Add Windows Proxy Target Applications and Accounts

You can manage credentials for Windows Proxy accounts. For introductory information about the Windows Proxy, see [Add a Windows Proxy Connector](#).

To configure Windows Proxy target applications and accounts, follow these procedures:

### Prerequisites for Windows Proxy Accounts

To register Windows Proxy target accounts, including Windows services, verify that the following prerequisites are met.

- [Install a Windows Proxy for Credential Manager](#) on the target server or another server in the domain that the target server can access.
- Create a Device (target server) of type Password Management or A2A.
- Verify that you have control of an account with Administrator rights on the target server.
- If the Windows Remote target account is of Administrator account type, the account requires Administrator rights on the Windows server.

**NOTE**

If your target account is to be used as a service account (that is, it is to be used to rotate passwords of other target accounts), we recommend that you prevent this account from being able to login interactively. To do this, assign the following User Rights to the Windows account:

- Deny log on locally
- Deny log on through Remote Desktop Service

**Create a Windows Target Application****Follow these steps:**

1. Select **Credentials, Manage Targets, Applications**. The Application List page appears.
2. Select **Add**. The Add Target Application page appears.
3. Select the **Host Name** magnifying glass to find an existing target server.
4. Enter a unique **Application Name**.
5. Select "Windows Proxy" as the **Application Type**.  
The Windows Proxy and Account Discovery tabs appear.
6. (Optional) Select a **Password Composition Policy**.
7. If you are using target groupings, add **Descriptors**.
8. On the **Windows Proxy** tab, select the **Account Type**.  
If you select **Local Account**, go to the next step. If you select **Domain Account**, you select from further options.
  - **Local Account** is only able to manage local accounts on target servers.
  - **Domain Account** is able to manage Windows Domain accounts. We recommend using the [Active Directory connector](#) to manage Domain Accounts.  
For the Domain Account, a drop-down list becomes active, with the following options:
    - **Target Server is Domain Controller** (For domain administrator accounts only)
    - **Domain Controllers are on servers** (with **Specify Servers** text field)  
Enter one or more servers, which are separated by commas.
    - **Lookup Domain Controllers in DNS**
    - **Lookup Domain Controllers in specified** (with **Specify DNS** text field)  
Enter one or more DNS servers, which are separated by commas
 For DNS Servers, complete the following fields:
    - **Domain Name**: Specify the Windows domain of the managed account
    - **Active Directory Site**: This field is not active for the Target Server is Domain Controller option. If you enter a value, it is used to narrow the search for domain controllers, using the specified name. If the field is empty, we search for all domain controllers in DNS.
    - **DC replication time (in ms)**: Enter the frequency of replication in milliseconds.
  - For **Active Directory Connect Timeout**, enter the timeout for connecting to AD, in milliseconds.
  - For **Active Directory Read Timeout**, enter the timeout for reading from AD, in milliseconds.
9. Select one or more **Available Proxies** and add them to the **Selected Proxies** list.
10. On the Account Discovery tab, select **Discover Services** and **Discover Tasks**. Specify an optional **Account Filter**.

**NOTE**

If you do not specify a filter, all accounts are discovered from the Windows server. Use only the \* character in filters. Example: User\*

11. Select **OK**.

The new Windows target application is added to the list of applications on the Target Applications page.

## Create a Windows Target Account and Target Alias

### Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**. The Account List page appears with a list of existing accounts.
2. Select **Add**. The Add Target Account page appears.
3. On the Account tab, select the magnifying glass to find an existing **Application Name** on the host server, or select + to create a target Application. Select or create a Windows Proxy type application.  
The **Host Name** field is filled. The Windows Proxy tab appears on the Add Target Account page.
4. Enter the **Account Name**. The Account Name must be unique for a given target application and must be the account name that is used by the target system.

### NOTE

This target account requires Administrator rights on the Windows server.

5. Select the **Password View Policy** for the account.
6. Select whether the **Account Type** is A2A (application-to-application) or privileged account. This choice is only possible if your license allows for A2A accounts.
7. (Optional) Enter an **Access Type**. Access type is a reference field for customer convenience. Access Type is not used by Credential Manager.
8. If you select A2A Account Type, more fields appear:
  - a. If you are using target groupings, enter **Descriptors** for the target Account.
  - b. Enter target **Aliases**. A target alias name must be unique across Credential Manager.
  - c. Enter the appropriate settings for password **Cache Behavior** for the A2A Client:
    - **Use Cache First:** The A2A Client looks for the password in local cache first. If there is no password or if the password is not the most recent, the A2A Client contacts Credential Manager.
    - **Use Server First:** The A2A Client contacts Credential Manager to get the most recent password. If a password is unavailable, the A2A Client looks in the local cache.
    - **No Cache:** The password is never stored in the local cache. The A2A Client always contacts Credential Manager for the password.
  - d. For A2A accounts that use caching, set the cache duration in **Cache Expiry Days**.
9. Enter an initial account **Password** or select the blue Generate Password icon to generate a default password. The Generate Password icon is to the right of the Password field, and looks like a ring with a set of keys.
10. On the Password tab, select **Discovery Allowed** to discover accounts from the Windows Proxy system.
11. Select the appropriate synchronization option (for example, update both Credential Manager and the target system). The **Synchronized** option is not available for the Generic application type.
  - **Update only the Password Authority Server:** Passwords are updated only in Credential Manager. Credential Manager and target system passwords can differ.
  - **Update both the Password Authority Server and the target system:** Password updates are performed both in Credential Manager and on the target system to maintain consistency.
12. If you use multiple target accounts, add the target servers on the Compound Servers tab. For more information, see the Compound Target Accounts section in [Add Target Accounts and Aliases](#).
13. (Optional) If you are adding or updating an account and you do not know the existing password, select the **Force password change** checkbox. The existing password gets changed, even though the account is not in sync.
14. Select **OK** to save changes.

Your new Windows Proxy Account is added to the Target Accounts page.

## Use An Alternate Account to Change Passwords

You can specify an account that has the authority to change passwords. On the Windows Proxy tab, the Change Process option lets you determine which account manages password changes. The options for this setting are:

- **Account can change own password.** To allow the existing target account to change its own password, keep the default option, **Account can change own password**, selected. The initial password that you enter must be the same as the target account password. The exception is a user with more privileges, who can update the password.
- **Use proxy credentials to change password.** Select this option for domain accounts. For this option to work:
  - Configure the Windows Proxy server on a Domain member.
  - Configure the service to run with credentials for a domain account that Windows Proxy connector can use to change passwords.
- **Use the following account to change password.** Select this option to specify a master account that can change password. For most target accounts, a blank field appears below the radio button. Select the magnifying glass and search for the target account to use as the alternate. Avoid using the current target account as the alternate. To show the target accounts that are defined in the system, filter by account name or host name. You can also show all target accounts. Typically, the other account is an account of the same application.

### **Discover Windows Proxy Target Account Services and Scheduled Tasks**

You can use account discovery to manage credentials of multiple Windows services and scheduled tasks. PAM can use the target account to manage changes and updates for any services and scheduled tasks that use this account. You do not have to update the password on an individual service or scheduled task basis.

#### **NOTE**

This procedure is for local Windows accounts. To discover services and scheduled tasks for Active Directory accounts, see [Discover Services and Scheduled Tasks for AD Accounts](#).

#### **Prerequisite**

Before you run account discovery, go to the Account Discovery tab of the Windows Proxy Target application. Select the discover option for services or tasks. You can select both.

#### **Discover Services and Tasks**

To discover new tasks and services on Windows Proxy accounts, follow these steps:

1. Select **Credentials, Discovery**.
2. On the Scan Profiles tab, select **Run** for the profile of the account you want to update.  
If a profile does not exist, follow these steps:
  - a. Select **Add**.
  - b. Give the profile a **Name**.
  - c. On the Servers tab, select the Server that is associated with the remote account.
  - d. Select **Run**.
3. Select the **Discovered Accounts** tab.  
Windows Proxy accounts that have updates available display a green checkbox under the Updates Available column.
4. Select the **Update** button for the Windows Proxy account with updates available.  
The Update Discovered Accounts window appears. Available Services and Scheduled Tasks appear on their respective tabs.
5. Select **OK**.
6. Select **Yes** when you are prompted to Update Selected Accounts.
7. To see a list of services and scheduled tasks:
  - a. Select **Credentials, Manage Targets, Accounts**.
  - b. Select the Services and Scheduled Tasks tabs to display the list accounts.

To remove tasks and services from a Windows Proxy Target Accounts, follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the account that you want to modify.

3. Select **Update**.
4. Select the Services or Scheduled Tasks tab.
5. To delete a service or task, select the **X** next to the entry.

**NOTE**

**More Information:** [Account Discovery](#)

## Windows Proxy Target Connector CLI Configuration

This section describes using the Credential Manager command-line interface (CLI) to add Windows Proxy applications and accounts. For introductory information about the Windows Proxy, see [Configure the Windows Proxy Connector](#).

### Windows Proxy Add Target Application CLI Parameters

To add a Windows Proxy target application and connector using the CLI, use the [addTargetApplication](#) command and the following command parameters:

#### ***Attribute.extensionType***

Specify the type of account to be used.

Required	Default Value	Valid Values
yes	N/A	windows

#### ***Attribute.agentId***

The identifiers for the Windows Proxies used to manage passwords.

Required	Default Value	Valid Values
yes	N/A	Comma separated list of Windows Proxy IDs. Each ID is a numeric.

#### ***Attribute.accountType***

The type of account being managed.

Required	Default Value	Valid Values
no	domain	domain, local

#### ***Attribute.domainName***

The Windows domain for the managed accounts.

Required	Default Value	Valid Values
Required if Attribute.accountType is set to domain (the default)	none	Domain name (a text string)

#### ***Attribute.domain***

The Windows domain for the managed accounts. This setting exists only for backwards compatibility. We recommend using `Attribute.domainName` instead.

Required	Default Value	Valid Values
Required if <code>Attribute.accountType</code> is set to domain (the default)	none	Domain name (a text string)

### ***Attribute.useDNS***

Determine the level to which DNS is used.

Required	Default Value	Valid Values
Required if <code>Attribute.accountType</code> is set to domain (the default)	none	One of: <ul style="list-style-type: none"> <li><code>noDNS</code> : DNS is not used</li> <li><code>retrieveDNS</code> : Retrieve the DNS server that is used by the Credential Manager server</li> <li><code>specifiedDNS</code> : Use the DNS server that is specified by the <code>dnsServer</code> attribute</li> </ul>

### ***Attribute.dnsServer***

The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if <code>Attribute.useDNS</code> is set to <code>specifiedDNS</code>	none	Comma separated list of DNS server host names.

### ***Attribute.specifiedServersList***

Provide a comma separated list of domain controllers.

Required	Default Value	Valid Values
Required if <code>Attribute.useDNS</code> is set to <code>specifiedServers</code>	none	Comma separated list of valid domain controllers.

### ***Attribute.adSite***

The Active Directory site. This parameter is only used if `Attribute.useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers using the specified name.

Required	Default Value	Valid Values
no	none	String.

## **Windows Proxy Add Target Account CLI Parameters**

To add a Windows Proxy target account that uses the target connector, use the [addTargetAccount](#) command and the following parameters:

### ***Attribute.extensionType***

Specify the type of account to be used.

Required	Default Value	Valid Values
yes	N/A	windows

#### ***Attribute.useOtherAccountToChangePassword***

Specify whether to use the target account or a different account to perform password change requests.

Required	Default Value	Valid Values
yes	N/A	true, false, agent

#### ***Attribute.otherAccount***

Specify which other account to use to perform password change requests.

Required	Default Value	Valid Values
Required if <code>Attribute.useOtherAccountToChangePassword</code> is true.	N/A	String. A valid target account ID.

#### ***Attribute.serviceInfo***

List services.

Required	Default Value	Valid Values
no	N/A	<code>&lt;empty string&gt;</code> no services Add the following attribute for each service: <code>&lt;hostname&gt;:&lt;servicename&gt;:restart</code> or <code>&lt;hostname&gt;:&lt;servicename&gt;:norestart</code> Multiple services are delimited by the   character. <code>&lt;hostname&gt;</code> is the name of the server where the service is hosted.

#### ***Attribute.tasks***

List scheduled tasks.

Required	Default Value	Valid Values
no	none	<code>&lt;empty string&gt;</code> no tasks Add the following attribute for each task: <code>&lt;hostname&gt;:&lt;taskname&gt;</code> Multiple services are delimited by the   character. <code>&lt;hostname&gt;</code> is the name of the server where the scheduled task is hosted.

#### ***Attribute.forcePasswordChange***

This parameter specifies whether Credential Manager updates passwords that fail verification during an initial synchronization. The default value is false. To update passwords that fail initial synchronization, set the attribute value to true.

Required	Default Value	Valid Values
no	false	true, false

### **Windows Proxy CLI Example**

```
cmdName=addTargetApplication TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myWindows

TargetApplication.type=windows Attribute.extensionType=windows Attribute.agentId=1

Attribute.accountType=domain Attribute.domainName=testDomain
```

```
cmdName=addTargetAccount TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=mywindows

TargetAccount.userName=admin TargetAccount.password=P@ssw0rd
TargetAccount.cacheAllow=true

TargetAccount.cacheDuration=19 Attribute.extensionType=windows
Attribute.useOtherAccountToChangePassword=false

Attribute.forcePasswordChange=false Attribute.serviceInfo=HostA:serviceName:restart|
HostB:ServiceName:norestart

Attribute.tasks=HostA:taskName|HostB:taskName
```

## **Windows Proxy Target Connector External API Configuration**

This topic describes the required and supported Attributes used when adding or updating Windows Proxy target applications using the External API.

### **Windows Proxy Target Application External API Parameters**

To add or update a Windows Proxy target application using the External API, use the following properties as members of the "attributes" associative array included in the 'body' parameter of the REST call.

#### ***agentId***



The identifiers for the Windows Proxies used to manage passwords.

Required	Default Value	Valid Values
Required if agentHostname is not set	N/A	Comma separated list of Windows Proxy IDs. Each ID is a numeric.

### ***agentHostname***

The host names of the Windows Proxies used to manage passwords.

Required	Default Value	Valid Values
Required if agentId is not set	N/A	Comma separated list of Windows Proxy Hostnames

### ***accountType***

The type of account being managed.

Required	Default Value	Valid Values
no	domain	domain, local

### ***domainName***

The Windows domain for the managed accounts.

Required	Default Value	Valid Values
Required if accountType is set to domain (the default)	none	Domain name (a text string)

### ***domain***

The Windows domain for the managed accounts. This setting exists only for backwards compatibility. We recommend using `domainName` instead.

Required	Default Value	Valid Values
Required if accountType is set to domain (the default)	none	Domain name (a text string)

### ***useDNS***

Determine the level to which DNS is used.

Required	Default Value	Valid Values
Required if accountType is set to domain (the default)	none	One of: <ul style="list-style-type: none"> <li><code>noDNS</code> : DNS is not used</li> <li><code>retrieveDNS</code> : Retrieve the DNS server that is used by the Credential Manager server</li> <li><code>specifiedDNS</code> : Use the DNS server that is specified by the <code>dnsServer</code> attribute</li> </ul>

***dnsServer***

The host names of the DNS servers to use.

Required	Default Value	Valid Values
Required if <code>useDNS</code> is set to <code>specifiedDNS</code>	none	Comma separated list of DNS server host names.

***specifiedServersList***

Provide a comma separated list of domain controllers.

Required	Default Value	Valid Values
Required if <code>useDNS</code> is set to <code>specifiedServers</code>	none	Comma separated list of valid domain controllers.

***adSite***

The Active Directory site. This parameter is only used if `useDNS` is set to `retrieveDNS` or `specifiedDNS`. If a value is given, Credential Manager uses the value to narrow the search for domain controllers using the specified name.

Required	Default Value	Valid Values
no	none	String.

**Windows Proxy CLI Example**

```
{
  "applicationName": "MyWindows",
  "applicationType": "windows",
  "attributes": {
    "agentId": "1",
    "accountType": "domain",
    "domainName": "testDomain"
  }
}
```

**View Windows Proxy Logs**

You can view Windows Proxy logs with the UI, so you can troubleshoot client issues.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Proxies**.
2. Select the host name of the server where the proxy whose logs you want to view is installed and select **Update**.

**NOTE**

You can only request the most recent log file. Previously rotated files are excluded.

3. Select the **Get Logs** button.

A zip file containing the Windows Proxy logs directory is downloaded to your browser. The default maximum file size is 20 MB. You can configure the maximum file size using the `getLogsMaxSize`

`{SystemProperty.SYSTEM_PROPERTY_MAX_LOG_SIZE}` property setting. For further details, see the description of the [setSystemProperty](#) CLI command.

## API Key Target Connector

This target connector is for the Privileged Access Manager External API. This connector does not map to any device, but it is available as an application type so an administrator can view the password. The API Key connector supports rollover of the target account, but there is no external device that needs its password rolled over.

The connector does not introduce any additional parameters when using the CLI to add a target application or target account.

## Develop Custom Connectors for Remote Targets

The out-of-the-box application types and target connectors that the appliance provides might not be sufficient for your remote systems and applications. For remote targets that are not available out-of-the-box, you can build custom target connectors. Privileged Access Manager offers a Custom Connector framework, which provides the necessary components to develop custom target connectors.

The process to build a custom target connector includes the following tasks:

- [Deploy the Custom Connector Software](#)
- [Try Out the Sample Custom Connectors](#)
- [Learn How to Use the Custom Connector Components](#)
- [Build Your Custom Connector](#)
- [Configure Custom Connectors Using the CLI](#)
- [Troubleshoot Custom Connector Issues](#)

Before you begin these tasks, familiarize yourself with the target connector framework.

### Target Connector Framework Functions

The *target connector framework* (TCF) and a custom connector enable users with the necessary privileges to view and update remote account passwords.

#### **NOTE**

The target connector framework is referred to as the **TCF** going forward in this guide.

The TCF communicates with the appliance and the custom target connector for the following functions:

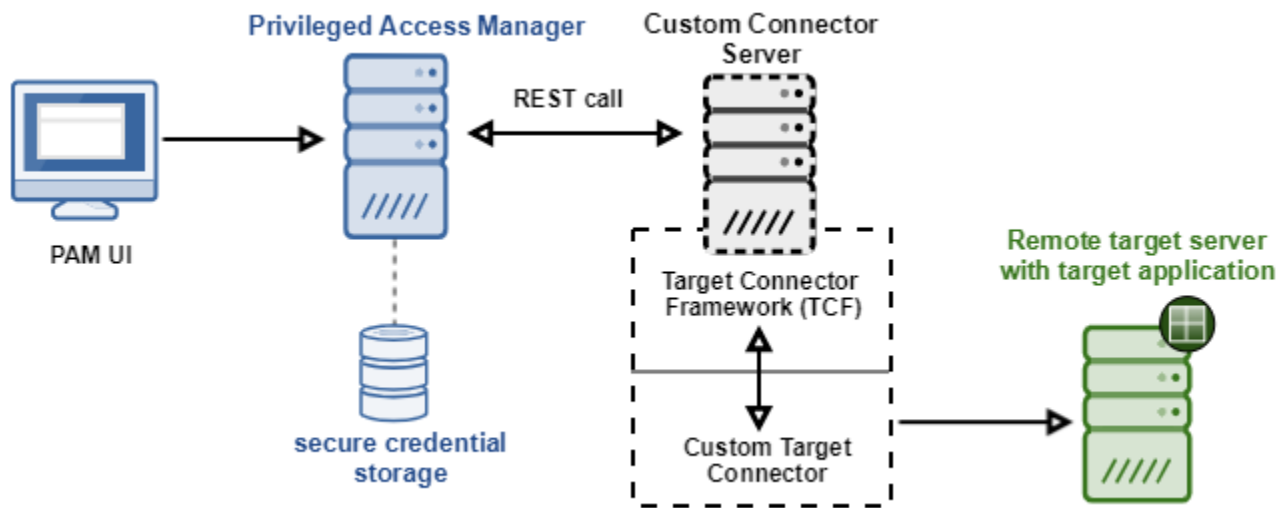
- Sends the appliance information about the custom connector and the remote target.
- Sends information about the target application and target account to the UI.
- Exchanges data between the appliance and the custom target connector to change and view the target account passwords.

The TCF and the custom target connector are installed on a *Custom Connector server*. The Custom Connector server is a Tomcat server.

#### **NOTE**

Any reference to the **Custom Connector server** implies a Tomcat server where the TCF and custom target connector are installed.

The following graphic shows where the TCF and custom connector reside in a PAM deployment.

**Figure 26: Custom Target Connector in a Network**

### **TCF Communication with PAM and Custom Connectors**

The TCF has the following main components:

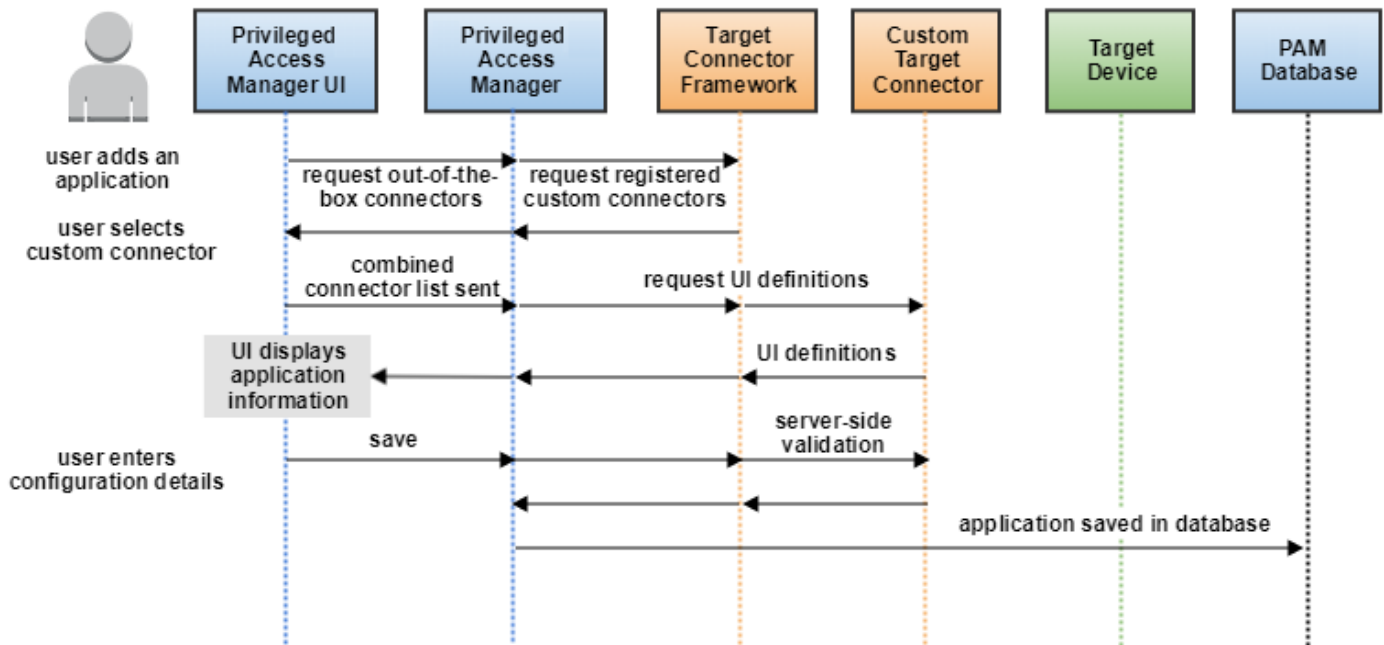
- TCF web application
- UI schema to define the custom UI fields and controls
- A TCF SDK

The TCF web application acts as a proxy between PAM and the custom target connectors. When the appliance sends a request for available target connectors, the TCF calls the custom target connectors. The TCF then sends the list of deployed connectors back to the appliance. The UI elements are then rendered on the appliance. The TCF also handles tasks that are related to verifying and changing account passwords. The TCF sends a request to the target connector to perform these tasks.

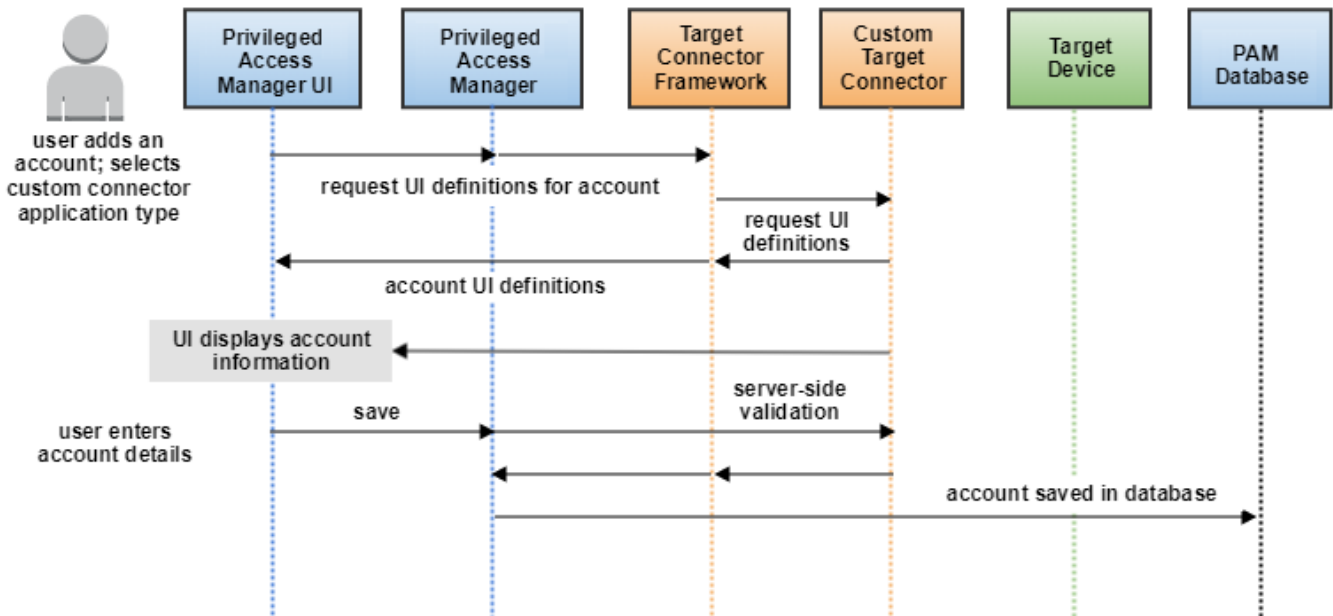
When a custom target connector starts up, it registers with the TCF. The connectors themselves manage the UI fields and controls for target accounts and applications.

### ***Data Flow for a Target Application***

The following graphic shows the data flow between Privileged Access Manager, the TCF, the target connector, and the target application:

**Figure 27: Target Connector Framework Data Flow****Data Flow for a Target Account**

The following graphic shows the data flow between PAM, the TCF, the target connector, and the target account:

**Figure 28: Target Connector Framework Account Data Flow**

## **Customer Responsibilities for Custom Connectors**

If you build custom target connectors that are based on the TCF, you are responsible for the operation between the custom target connector and the target endpoint. These responsibilities include:

- Writing log messages from the target connector to the TCF server catalina.out log
- Writing any log messages that the target connector returns to PAM.
- Obfuscating passwords when log messages are written into the catalina.out file on the TCF server.
- Providing for secure information transfer between the target connector and the target endpoint.

CA Technologies is responsible for operation up to the point where the TCF passes information to the custom target connector. After that point, you are responsible for how the custom connector handles communication, operationally and securely.

### **NOTE**

**Begin the first task:** [Deploy the Custom Connector Software](#).

## **Deploy the Custom Connector Software**

This topic explains how to install and deploy the Custom Connector software. The procedures apply to development and production systems, with one more step for the production system. After deployment on a production system, you remove two folders.

### **NOTE**

In this topic, example file paths are for UNIX systems and use a forward slash (/). For Windows systems, the paths are similar but use a backward slash (\).

## **Required Software for the Custom Connector Server**

The Custom Connector Server (Tomcat) server needs the following software:

- Apache Tomcat 9
- Java 8 or Java 11 (In a deployed production environment, you only need the JRE)

## **Minimum System Requirements**

- 2 CPUs are recommended but 1 CPU is sufficient
- 4-GB RAM
- 32-GB Disk space

## **Install Tomcat**

Install Tomcat 9 on a Windows or Linux system. If you install Tomcat on a Linux system, run Tomcat as a service. For installation instructions, see the [Apache Tomcat 9 documentation](#).

### **WARNING**

Use a dedicated Tomcat server for the Custom Connector installation.

## **Download the Custom Connector Software**

Download the Custom Connector software from the Broadcom Support site to the Tomcat server that you created. For information on how to download the software, see [Download PAM Installation Media](#).

### **NOTE**

The Tomcat server is referred to as the *Custom Connector Server* throughout the rest of the documentation.

## ***Extract the Custom Connector Files***

Unzip the Custom Connector archive to a directory, such as **/tmp/tcf**. The subdirectories and files that are shown in the following table are created under that directory:

Directory	Content
<b>application</b>	<code>capamef.war</code> : The TCF web application.
<b>conf</b>	<ul style="list-style-type: none"> <li><code>capamef_messages.properties</code> : Contains messages for the framework to report in tomcat log and potential back to when problems occur</li> <li><code>extension_framework.properties</code> : A set of configuration properties the framework uses to communicate with the core pieces of the extension framework running in Tomcat and PAM.</li> </ul>
<b>samples</b>	<ul style="list-style-type: none"> <li><code>exampleTargetConnector.war</code> : Sample target connector for Linux devices</li> <li><code>echoTargetConnector.war</code> : Sample target connector which logs received requests.</li> </ul>
<b>sdk</b>	<ul style="list-style-type: none"> <li><code>lib</code> : Contains the library <code>caextensionscore-x.xx.x.jar</code> and its dependencies. The <code>x.xx.x</code> represents the version of the JAR.</li> <li><code>customConnectorTemplate</code> : Contains project metadata files that are related to the tools Gradle, Maven, and the source code.</li> <li><code>exampletargetconnector</code> : Contains the source code for the Example Target Connector.</li> <li><code>echotargetconnector</code> : Contains the source code for the Echo Target Connector.</li> <li><code>createTCProject</code> : A shell script for UNIX platforms to create the custom connector project.</li> <li><code>createTCProject.cmd</code> : A batch script for Windows systems to create the custom connector project.</li> <li><code>tcProjectGenerator.jar</code> : The library that generates the custom connector project.</li> </ul>
<b>configTCF</b>	<p>Tools for various TCF encryption tasks:</p> <ul style="list-style-type: none"> <li><code>capamextensionstcfCryptoUtil-x.xx.x.jar</code> : A library that encrypts and decrypts the keystore password. The library uses the Machine ID of the system where the Custom Connector server is installed. The <code>x.xx.x</code> represents the version of the JAR.</li> <li><code>configTCF</code> : The UNIX utility for creating a keystore for encryption and decryption tasks.</li> <li><code>configTCF.cmd</code> : The Windows utility for creating a keystore for encryption and decryption tasks.</li> </ul>

### **Deploy the Custom Connector WAR Files**

To deploy the Custom Connector WAR files on the Custom Connector Server, the directories and WAR files must have the right owners and permissions. The required file and directory ownership and permissions are listed by platform:

#### **Linux Platforms**

- **File and Directory Ownership:** Set the owner to the Tomcat user and group. For example, to set the ownership of the `capamef.war` enter:

```
chown tomcat:tomcat capamef.war
```

- **File Permissions:** Give the Tomcat user read/write permissions. For example, to set the permissions for capamef.war, enter:

```
chmod 600 capamef.war
```

- **Directory Permissions:** Give the Tomcat user Read/Write/Execute (rwx) permissions. Give the group Read/Execute (rx) permissions. For example, to assign rx permissions to the webapps\_targetconnectors directory, enter:

```
chmod 750 webapps_targetconnectors
```

## Windows Platforms

- **File and Directory Ownership:** The Windows Administrator must be the owner
- **File and Directory Permissions:** Only the Administrator user from the group Administrators has write access. No other user has write permissions.

## Deploy the WAR files

### Follow these steps:

1. Copy the **capamef.war** file to the directory */CATALINA\_HOME/webapps*, where *CATALINA\_HOME* is the installed location of the server.
2. Under the *CATALINA\_HOME*, create a directory that is named **webapps\_targetconnectors**.
3. Copy the **exampleTargetConnector.war** file and the **echoTargetConnector.war** file to the **webapps\_targetconnectors** directory.
4. Configure the Custom Connector server, as instructed in the next section.

## Configure the Custom Connector Server

After you deploy the software, complete the following tasks at the Custom Connector server:

1. Create a keystore for HTTPS communication
2. Modify the server.xml file

In the following procedures, *CATALINA\_HOME* is the installed location of the server.

### Create a Keystore for HTTPS Communication

For secure communication between PAM and the TCF, configure the Tomcat server to use TLS. This step is optional but recommended. For TLS support, create a keystore with a keystore password. The keystore holds the X.509 key/certificate pair for securing communication. For complete instructions about configuring TLS, see the Apache Tomcat documentation.

To secure the keystore, encrypt the keystore password. Use the Custom Connector server utility, named **configTCF**, to encrypt the keystore password. The password is encrypted with the Machine ID of the system on which the Custom Connector server is installed. Each system has a unique Machine ID.

The following procedure uses the keytool utility as an example. You can create a keystore using other tools.

### To create a keystore and encrypt the password, follow these steps:

1. Create a PKCS12 keystore by entering the following keytool command. The keystore must contain an X.509 private key and certificate pair in PEM format.

```
keytool -genkey -alias pam -keyalg RSA -keysize 2048 -storetype PKCS12 -dname
"CN=capamtcf,OU=PAM,O=Organization,L=City,ST=State,C=Country" -keypass keystore_password -
storepass keystore_password -keystore keystore_file -validity 360
```

*Organization* is the name of the organization. For example, "Broadcom".

*City* is the name of city in which the keystore is located. For example, "Burlington".

*State* is the code for the state or province in which the keystore is located. For example, "MA".

*Country* is the code for the state or province in which the keystore is located. For example, "US".



*keystore\_password* is the password that you want to assign to the keystore.

*keystore\_file* is full path and file name of the location that you want to generate the keystore.

2. Give the user running the Tomcat process **read** permission to the keystore file.
3. Extract the certificate from the keystore that you generated in step 1 by executing the following command:

```
keytool -exportcert -alias pam -keystore keystore_file -keypass keystore_password -storepass keystore_password -rfc -file tcf.crt
```

Keep the file tcf.crt. This certificate is required when you configure the PAM Custom Connector settings later.

4. Navigate to the location of the extracted TCF zip file and find the **configTCF** folder.
5. Encrypt the keystore password by executing the command for your operating system:

– **Windows:**

```
configTCF.cmd -Dcommand=encryptPassword -Dpassword=keystore_password
```

– **Unix/Linux:**

```
configTCF -Dcommand=encryptPassword -Dpassword=keystore_password
```

*keystore\_password* is a password value that you assigned.

The configTCF command output is an encrypted keystore password that is displayed on the command prompt.

6. Copy the encrypted password to a temporary file.
7. From the configTCF folder, copy the **capamextensionstcfCryptUtil.jar** file to *CATALINA\_HOME/lib*. *CATALINA\_HOME* is the location where the Tomcat server is installed.
8. Navigate to *CATALINA\_HOME/conf* and open the **catalina.properties** file.
9. Copy the following line from this document and paste it at the end of the **catalina.properties** file:

```
org.apache.tomcat.util.digester.PROPERTY_SOURCE=com.ca.pam.extensions.tcfcryptoutil.TCFPropertySource
```

*encrypted\_keystore\_password* is the encrypted password that is generated in the previous step.

The encrypted keystore password is unique to the system where it is generated. You cannot generate the password on one server then copy the encrypted information to another server. On each production server, run the configTCF to encrypt the keystore password. After the password is encrypted, delete the configTCF utility from the system.

## NOTE

An alternate method to secure the keystore is to use the PAM A2A functionality. For instructions, see [Use A2A to Secure the Keystore for HTTPS \(Optional\)](#).

## Modify the Tomcat server.xml File

Modify the server.xml file to:

- Add a connector service that uses port 18080 (required)
- Add a connector service that uses port 8443 for HTTPS communication (required only for TLS support)

## Follow these steps:

1. Navigate to */CATALINA\_HOME/bin* and enter values for the required variables in the catalina.sh script.
2. Navigate to */CATALINA\_HOME/conf*.
3. Copy the **server.xml** file then rename the *original* file. Give the original file a unique name.
4. Open the server.xml file in a text editor.
5. Add a connector service that uses port 18080. **This port uses loopback address 127.0.0.1 for IPv4 and ::1 for IPv6.** The following file excerpt shows an example of the added connector service (CatalinaTC):

```
<Service name="CatalinaTC">
  <Connector port="18080" protocol="HTTP/1.1" connectionTimeout="30000"
    URIEncoding="UTF-8" address="127.0.0.1" />
  <!-- Define an AJP 1.3 Connector on port 8009
    <Connector port="18009" protocol="AJP/1.3" redirectPort="18443" />
  <Engine name="CatalinaTC" defaultHost="targetconnectors">
    <Host name="targetconnectors" appBase="webapps_targetconnectors"
```

```

    unpackWARs="true" autoDeploy="false" deployOnStartup="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
    prefix="localhost_access_log" suffix=".txt"
    pattern="%h %l %u %t &quot;%r&quot; %s %b" />
  </Host>
</Engine>
</Service>

```

For an IPv6 IP address, the third line below should be used:

```

<Service name="CatalinaTC">
  <Connector port="18080" protocol="HTTP/1.1" connectionTimeout="30000"
  URIEncoding="UTF-8" address="::1" />
  ...

```

6. Keep port 8080 open for the local host at least. To ensure port 8080 is open, verify that *one* of the following entries is in the server.xml file, under:

If you enabled TLS for the Custom Connector, ensure that the following entry exists:

```

<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="30000" URIEncoding="UTF-8"
address="127.0.0.1" />

```

If you did not enable TLS, ensure that the following entry exists:

```

<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="30000" URIEncoding="UTF-8"/>

```

7. If you enable TLS for the Custom Connector, add a connector service that uses port 8443 (HTTPS port). Add this connector under the default Catalina service (<Service name="Catalina">) section. Port 8080 is in the server.xml file by default; but use port 8443 for secure TCF communication.

The following code excerpt shows how to add port 8443:

```

<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="keystore_file_path" keyAlias="unique_key_identifier" keystorePass="${tomcat.keystore.pwd}"
clientAuth="false" sslProtocol="TLS" xpoweredBy="false"/>

```

Ensure that you specify the full keystore file path, including the name of the keystore.

#### TIP

Enter the string `keystorePass="${tomcat.keystore.pwd}"` exactly as shown. This string is an alias for the encrypted password. Use the `keyAlias` attribute to uniquely identify the key to avoid identification issues when there are multiple keys in the keystore.

8. Save the server.xml file.
9. Restart the Tomcat server.
10. Verify that the Tomcat server is set up correctly. Navigate to `CATALINA_HOME/logs` and look for the following messages:

```

INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-8080"]
INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["https-jsse-nio-8443"]
INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-127.0.0.1-18080"]
INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-
nio-0:0:0:0:0:0:0:1-18080"]
INFO [main] org.apache.catalina.startup.Catalina.start Server startup in <duration_to_start_server>

```

If the Tomcat server does not start up, see [Troubleshoot Custom Connector Issues](#) for possible solutions.

## Secure the Custom Connector Server

We recommend that you harden, that is, secure the Custom Connector server. Securing the server reduces its vulnerability to attacks. For instructions on how to [secure the Tomcat server](#), see the Tomcat documentation. See also the [sample server.xml file](#), which has entries for securing the server.

## Configure Custom Connector Settings at PAM

The Custom Connector configuration page has settings to identify the Custom Connector server. The page also has settings to secure communication between PAM and the Custom Connector server.

### Follow these steps at the PAM UI:

1. Log in to the PAM UI and navigate to **Configuration, Custom Connectors**.
2. Identify the Custom Connector server by entering values for the following fields:
  - **Server Address**: Enter the IP address of the Tomcat server
  - **Server Port**: Enter the port on which Tomcat listens for HTTP traffic
3. Specify the timeout settings:
  - **Connect Timeout (sec)**: This timeout specifies how long PAM waits for a response from the TCF. Default: 3 seconds
  - **Read Timeout (sec)**: This timeout specifies how long PAM waits for a response from TCF. This timeout is for requests other than credential management operations, such as requests for data to construct and validate the UI content. Default: 3 seconds.
  - **Update Timeout (sec)**: This timeout specifies how long PAM waits for a response from the TCF about credential management operations. Operations can include a password verification or a password rollover. Default: 30 seconds
4. (Optional but recommended) Enable TLS to secure the communication channel:
  - a. Obtain the server certificate (**tcf.crt file**) from the Custom Connector server keystore. You extracted the tcf.crt file after you [created a keystore for HTTPS communication at the Tomcat server](#).
  - b. Confirm that the **Use TLS** checkbox is selected. We recommend using TLS over HTTPS port 8443.
  - c. For the **Certificate Filename** field, select **Choose File** next to the field. Browse to the server certificate on your local system and select it. The file name displays in the **Current Certificate File** field.
5. Generate an encryption key. The key encrypts the authentication token and the payload that PAM sends with each REST call to the Custom Connector server.
  - a. Next to the **Encryption Key** field, select **Generate Key**. The appliance creates a key and puts the value in the field. For example: **em6/C5X7GxBZiGt9QF4Z56SBjxOM2jvmwoacGjUAXvk=**
  - b. Copy the encryption key value and save it to a file.
  - c. For the **Authentication Token Validity (sec)** field, determine how long you want the authentication token to be active. The default value (120 seconds) allows for any timing delays between PAM and the Custom Connector server. The PAM and Custom Connector servers clocks must be synchronized.
6. Select **Save**. A message indicates that the appliance is connected to the Custom Connector server.

### WARNING

The **Clear** button returns the settings on the page to the factory defaults. The Clear button also deletes your configuration from the UI and the PAM database. To reestablish your configuration, you must regenerate the encryption key. Finally, copy the new values over to the `extension_framework.properties` file on the Custom Connector server.

## Create a Keystore at the Custom Connector Server

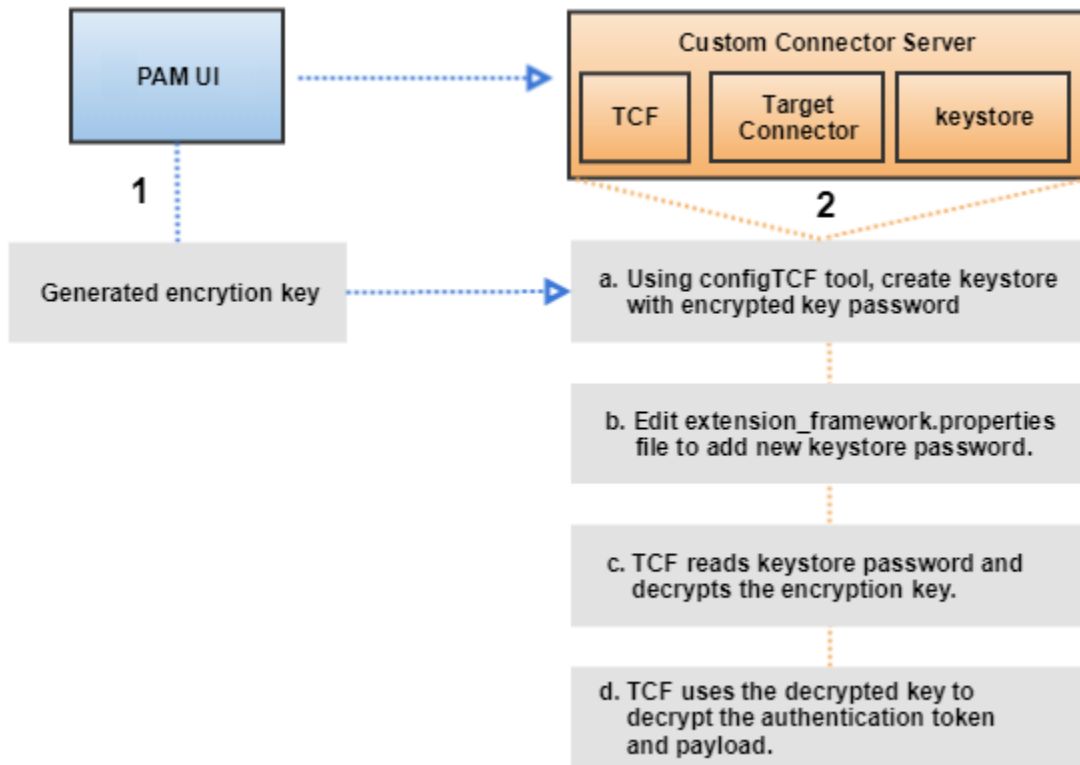
During a REST call to the Custom Connector server, PAM sends an encrypted authentication JWT token in the header and an encrypted payload. Store the encryption key in a keystore at the Custom Connector server. To authenticate a request, the TCF decrypts the JWT token using the stored encryption key. If the TCF cannot decrypt the token, it rejects the request. If decryption is successful, it then uses the key to decrypt the payload.

To generate a keystore, run a configuration utility at the Custom Connector server.

**NOTE**

The keystore that holds the encryption key is unique from the keystore that holds X.509 key/certificate pair for HTTPS communication.

The following graphic illustrates the PAM payload encryption process:

**Follow these steps:**

1. Create a directory named **tcf** in the location `/$CATALINA_HOME/tcf`. The tomcat user should own this directory. Permissions to access this directory should be and have Read/Write/Execute (rwx) for the Tomcat user and Read/Execute (rx) for users in the Tomcat group.
2. Create a keystore. Use the **configTCF** command (UNIX) or **configTCF.cmd** (Windows) and the PAM-generated encryption key. The command syntax is:

```
configTCF -Dcommand=createKeyStore -DkeyStoreFile=keystore_path_and_name -
DkeyStorePW=user_assigned_password -Dkey=CAPAM_encryption_key
keystore_file: file path and name of the keystore.
```

**keystore\_path\_and\_name:** The location and name of the keystore on the Tomcat server.

**user\_assigned\_password:** The password that you specify for the keystore **CAPAM\_encryption\_key:** The key that is generated at the PAM UI and copied to this command

**Windows example:**

```
configTCF.cmd -Dcommand=createKeyStore -DkeyStoreFile="%CATALINA_HOME%\tcf\keyStore -
DkeyStorePWD=keypwd -Dkey=em6/C5X7GxBZiGt9QF4Z56SBjxOM2jvmwoacGjUAXvk=
```

**UNIX example:**

```
configTCF -Dcommand=createKeyStore -DkeyStoreFile=/$CATALINA_HOME/tcf/keyStore -DkeyStorePWD=keypwd -
Dkey=em6/C5X7GxBZiGt9QF4Z56SBjxOM2jvmwoacGjUAXvk=
```

After this configTCF command executes, the file `keyStore` is created in the directory `CATALINA_HOME/tcf/keyStore` and the key password (`keypwd`) is encrypted. The encrypted value of the password `keypwd` is `PIdadRtvyRGPOlCSU7lSxWGgbpnyadRMA5q6cMagx2U=`.

#### NOTE

If you do not specify a file path, the keystore file is created in the directory from where you execute the `configTCF` command.

3. Copy and save the encrypted key store password.
4. Give the user running the Tomcat process **read** permission to the keystore file.
5. Navigate to the **extension\_framework.properties** file at `CATALINA_HOME/webapps/capamef/WEB-INF/classes/extension_framework.properties`.
6. Edit the properties file and add the following entries:
  - `extension.encrypted.pwd`: copy the new password that was generated by the configTCF tool.
  - `extension.keystore.file`: specify the path of the keystore.

If Tomcat's `server.xml` uses `::1` as a loopback address, then modify the `extension.url.prefix` as follows:  
`extension.url.prefix=http://[::1]:18080`
7. If tomcat's `server.xml` uses `::1` as a loopback address, then navigate to `CATALINA_HOME/conf` and open the `catalina.properties` file. Copy the following line from this document and paste it at the end of the `catalina.properties` file:  
`tomcat.tcf.ipv6.preferred=true`
8. The following example shows the new properties in bold. The values of these properties are from the executed configTCF command.

```
Connector.name=TargetConnectorRegistry
extension.url.prefix=http://127.0.0.1:18080
extension.connection.timeout=100000
extension.read.timeout=100000
extension.encrypted.pwd=PIdadRtvyRGPOlCSU7lSxWGgbpnyadRMA5q6cMagx2U=
extension.keystore.file=/home/tcf/keyStore
```

#### WARNING

On Windows and UNIX platforms, always use forward slashes (/) for file paths in the properties file.

9. Save the properties file.
10. Restart the Tomcat server.

To decrypt the token and payload, the TCF reads the **extension.encrypted.pwd** value from the `extension_framework.properties` file. The TCF uses the password to open the keystore and retrieve the encryption key. The key itself is decrypted, then TCF uses it to decrypt the token and payload. Finally, TCF sends the payload to the custom connector.

### Test the Deployment

To test the **communication between PAM to Custom Connector server**:

1. Log in to the UI and navigate to **Configuration, Custom Connectors**.
2. Select **Test** to verify that you can connect to the Custom Connector server.

If the connection is not working, you can also see a message at the top of the **Dashboard Overview Tab**.

**To verify that all files and sample target connectors are deployed correctly:**

1. Log in the PAM UI as a Global Administrator or Configuration Manager.
2. Select **Configuration** on the top menu.
3. Verify that you see the **Custom Connectors** option in the left pane.
4. Select **Credentials, Manage Targets, Application**.

5. Select **Add**.
6. In the **Application Type** field, confirm that the pull-down list includes the Echo Target Connector and Example Target Connector.
7. If you select either of the sample application types, a new tab displays for the application, such as **Example – Application**.
8. Exit from the UI.
9. Log in to the Custom Connector server where the TCF is deployed. Open the **catalina.out** file and look for a message that reads:

```
Registering client of type, targetConnectors, with name: echoTargetConnector
```

If you see the prior message, the deployment is successful.

### **Remove Unused Folders from the Production Systems**

After you deploy the Custom Connector on a production server, remove the following folders that are not required for use in production:

- sdk folder
- configTCF folder

### **Sample server.xml File**

The following code shows an example server.xml file, which has entries for securing a PAM server that can be used as a basis for securing the custom connector server.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "Server" is not itself a "Container", so you may not
define subcomponents such as "Valves" at this level.
Documentation at /docs/config/server.html
-->
<Server port="-1" shutdown="nondeterministic">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
  <!-- Security listener. Documentation at /docs/config/listeners.html
  <Listener className="org.apache.catalina.security.SecurityListener" />
  -->
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <!-- Prevent memory leaks due to use of particular java/javax APIs-->
```

```

<Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
<Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
<Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />

<!-- Global JNDI resources
    Documentation at /docs/jndi-resources-howto.html
-->
<GlobalNamingResources>
    <!-- Editable user database that can also be used by
        UserDatabaseRealm to authenticate users
    -->
    <Resource name="UserDatabase" auth="Container"
        type="org.apache.catalina.UserDatabase"
        description="User database that can be updated and saved"
        factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
        pathname="conf/tomcat-users.xml" />
</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share
    a single "Container" Note: A "Service" is not itself a "Container",
    so you may not define subcomponents such as "Valves" at this level.
    Documentation at /docs/config/service.html
-->
<Service name="Catalina">

    <!--The connectors can use a shared executor, you can define one or more named thread pools-->
    <!--
    <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
        maxThreads="150" minSpareThreads="4"/>
    -->

    <!-- A "Connector" represents an endpoint by which requests are received
        and responses are returned. Documentation at :
        Java HTTP Connector: /docs/config/http.html
        Java AJP Connector: /docs/config/ajp.html
        APR (HTTP/AJP) Connector: /docs/apr.html
        Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" xpoweredBy="false"/>

    <Connector
        protocol="org.apache.coyote.http11.Http11NioProtocol"
        port="8443" maxThreads="200"
        scheme="https" secure="true" SSLEnabled="true"
        keystoreFile="C:/pam/test/pam.pfx" keystorePass="firewall"
        clientAuth="false" sslProtocol="TLS" xpoweredBy="false"/>
    <!-- A "Connector" using the shared thread pool-->
    <!--
    <Connector executor="tomcatThreadPool"
        port="8080" protocol="HTTP/1.1"

```

```

        connectionTimeout="20000"
        redirectPort="8443" />
-->
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
This connector uses the NIO implementation. The default
SSLImplementation will depend on the presence of the APR/native
library and the useOpenSSL attribute of the
AprLifecycleListener.
Either JSSE or OpenSSL style configuration may be used regardless of
the SSLImplementation selected. JSSE style configuration is used below.
-->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
        maxThreads="150" SSLEnabled="true">
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
            type="RSA" />
    </SSLHostConfig>
</Connector>
-->
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443 with HTTP/2
This connector uses the APR/native implementation which always uses
OpenSSL for TLS.
Either JSSE or OpenSSL style configuration may be used. OpenSSL style
configuration is used below.
-->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol"
        maxThreads="150" SSLEnabled="true" >
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
    <SSLHostConfig>
        <Certificate certificateKeyFile="conf/localhost-rsa-key.pem"
            certificateFile="conf/localhost-rsa-cert.pem"
            certificateChainFile="conf/localhost-rsa-chain.pem"
            type="RSA" />
    </SSLHostConfig>
</Connector>
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
Documentation at /docs/config/engine.html -->

<!-- You should set jvmRoute to support load-balancing via AJP ie :
<Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
-->
<Engine name="Catalina" defaultHost="localhost">

```



```

<!--For clustering, please take a look at documentation at:
    /docs/cluster-howto.html (simple how to)
    /docs/config/cluster.html (reference documentation) -->
<!--
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->

<!-- Use the LockOutRealm to prevent attempts to guess user passwords
    via a brute-force attack -->
<Realm className="org.apache.catalina.realm.LockOutRealm">
    <!-- This Realm uses the UserDatabase configured in the global JNDI
        resources under the key "UserDatabase". Any edits
        that are performed against this UserDatabase are immediately
        available for use by the Realm. -->
    <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
        resourceName="UserDatabase"/>
</Realm>

<Host name="localhost" appBase="webapps"
    unpackWARs="true" autoDeploy="false">

    <!-- SingleSignOn valve, share authentication between web applications
        Documentation at: /docs/config/valve.html -->
    <!--
    <Valve className="org.apache.catalina.authenticator.SingleSignOn" />
    -->

    <!-- Access log processes all example.
        Documentation at: /docs/config/valve.html
        Note: The pattern used is equivalent to using pattern="common" -->
    <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
        prefix="localhost_access_log" suffix=".txt"
        pattern="%h %l %u %t &quot;%r&quot; %s %b" />
    <!--Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false"
        showServerInfo="false" /-->

</Host>
</Engine>
</Service>
<Service name="CatalinaTC">

<!--The connectors can use a shared executor, you can define one or more named thread pools-->
<!--
<Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
    maxThreads="150" minSpareThreads="4"/>
-->

<!-- A "Connector" represents an endpoint by which requests are received
    and responses are returned. Documentation at :
    Java HTTP Connector: /docs/config/http.html
    Java AJP Connector: /docs/config/ajp.html

```

```

    APR (HTTP/AJP) Connector: /docs/apr.html
    Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
-->
<Connector port="8080" protocol="HTTP/1.1"
    address="127.0.0.1" connectionTimeout="20000"
    redirectPort="8443" xpoweredBy="false"/>
<Connector port="8080" protocol="HTTP/1.1"
    address="0:0:0:0:0:0:0:1" connectionTimeout="20000"
    redirectPort="8443" xpoweredBy="false"/>

<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
    port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
-->

<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
    This connector uses the NIO implementation. The default
    SSLImplementation will depend on the presence of the APR/native
    library and the useOpenSSL attribute of the
    AprLifecycleListener.
    Either JSSE or OpenSSL style configuration may be used regardless of
    the SSLImplementation selected. JSSE style configuration is used below.
-->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true">
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
            type="RSA" />
    </SSLHostConfig>
</Connector>
-->

<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443 with HTTP/2
    This connector uses the APR/native implementation which always uses
    OpenSSL for TLS.
    Either JSSE or OpenSSL style configuration may be used. OpenSSL style
    configuration is used below.
-->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol"
    maxThreads="150" SSLEnabled="true" >
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
    <SSLHostConfig>
        <Certificate certificateKeyFile="conf/localhost-rsa-key.pem"
            certificateFile="conf/localhost-rsa-cert.pem"
            certificateChainFile="conf/localhost-rsa-chain.pem"
            type="RSA" />
    </SSLHostConfig>
</Connector>
-->

```

```

<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
Documentation at /docs/config/engine.html -->

<!-- You should set jvmRoute to support load-balancing via AJP ie :
<Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
-->
<Engine name="CatalinaTC" defaultHost="tclocalhost">

<!--For clustering, please take a look at documentation at:
/docs/cluster-howto.html (simple how to)
/docs/config/cluster.html (reference documentation) -->
<!--
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->

<!-- Use the LockOutRealm to prevent attempts to guess user passwords
via a brute-force attack -->
<Realm className="org.apache.catalina.realm.LockOutRealm">
<!-- This Realm uses the UserDatabase configured in the global JNDI
resources under the key "UserDatabase". Any edits
that are performed against this UserDatabase are immediately
available for use by the Realm. -->
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"/>
</Realm>

<Host name="tclocalhost" appBase="webapps_targetconnectors"
unpackWARs="true" autoDeploy="false">

<!-- SingleSignOn valve, share authentication between web applications
Documentation at: /docs/config/valve.html -->
<!--
<Valve className="org.apache.catalina.authenticator.SingleSignOn" />
-->

<!-- Access log processes all example.
Documentation at: /docs/config/valve.html
Note: The pattern used is equivalent to using pattern="common" -->
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %u %t &quot;%r&quot; %s %b" />
<!--Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false"
showServerInfo="false" /-->

</Host>
</Engine>
</Service>
</Server>

```

## Use an Alternate Custom Connector Server for Disaster Recovery

In a multi-site cluster environment, you can configure an alternate Custom Connector Server to be used if your primary site fails and a secondary site is promoted to be the new primary. The alternate Custom Connector Server configuration is replicated to all other members of the cluster but ignored until the **Use Alternate Server** option is set.

### NOTE

Although the alternate Custom Connector Server configuration is replicated to all other members of the cluster, the value of the **Use Alternate Server** setting, which controls whether the alternate Custom Connector Server is used, is not replicated. You must configure it independently on each node in the cluster.

Because credential management work with the Custom Connector Servers is done by the primary site, the Custom Connector Server specified on the secondary nodes (with the **Use Alternate Server** setting) is ignored until the secondary site becomes a primary site.

Also, because this setting is not replicated, you can select **Use Alternate Server** on the secondary site nodes in preparation for a potential secondary site promotion to primary site in the future. Credential management work with the Custom Connector Servers is done by the primary site. In that sense, the Custom Connector Server chosen on the secondary nodes ( the Use Alternate Server setting ) does not come into play until the secondary site becomes a primary site.

In a single-site environment, you can set up an alternate Custom Connector Server as a backup server. The alternate Custom Connector server uses a different TCF instance from the first instance that the main server uses. If your main server becomes inoperative for any reason, you can enable the already configured alternate Custom Connector Server for communication with your custom target connectors and applications.

### NOTE

All target connectors must be configured for each Custom Connector server instance.

### To configure an alternate server for disaster recovery (multi-site cluster):

1. At the primary site, navigate to **Configuration, Custom Connector**.
2. On the **Connector Server** panel, complete the settings then save the configuration.
3. Log in to a secondary site member.
4. On the **Connector Server** panel, set the **Use Alternate Server** option.
5. Select the **Alternate Connector Server** tab.
6. Configure the settings then save the configuration.
7. Repeat this procedure for each member of the secondary site.

If you promote the secondary site to become the primary, the configuration of the alternate Custom Connector Server is used.

### To configure an alternate server for manual backup (non-clustered environment):

1. From the UI, navigate to **Configuration, Custom Connector**.
2. Complete *one* of the following procedures:
  - If the Connector Server is not configured:**
    - a. Complete the settings then save the configuration.
    - b. Set the **Use Alternate Server** option then select the **Alternate Connector Server** tab.
    - c. On the **Alternate Connector Server** panel, configure the settings then save the configuration.
    - d. Return to the Connector Server
    - e. Unset the **Use Alternate Server** checkbox then save the configuration. Saving the changes updates the configuration to use the primary server.
  - If the Connector Server is configured:**
    - a. Set the **Use Alternate Server** option.
    - b. Select the **Alternate Connector Server** tab, configure the settings then save the configuration.

- c. Return to the Connector Server
- d. Unset the **Use Alternate Server** checkbox then save the configuration. Saving the changes updates the configuration to use the primary server.

If the Connector Server fails in production, log in to this server and set the **Use Alternate Server** option. This action makes the configured alternate server active and the first server inactive.

## Use A2A to Secure the Keystore and Password (Optional)

The Custom Connector keystore contains the TLS key/certificate pair for HTTPS communication. You can configure PAM to encrypt and store the keystore password. The Custom Connector server securely retrieves the password using the PAM A2A feature.

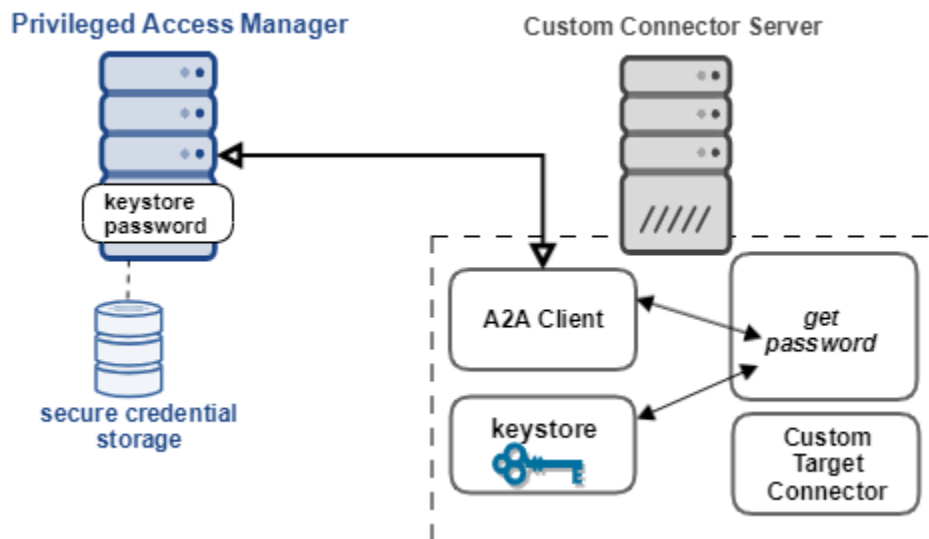
To implement the A2A method, configure specific target applications and associated A2A target accounts. The target accounts represent the password for accessing the keystore, a call stack hash, and a file list hash. These mechanisms work together to secure the keystore password. PAM can randomly generate the keystore password, which is used when you create the keystore at the Custom Connector server. The call stack and file list hashes ensure that the Custom Connector server, running in a trusted environment, retrieves the keystore password from PAM.

### NOTE

This A2A method is an alternative to using the `tcfCryptoUtil` utility to encrypt the keystore password. The A2A method provides file integrity validation, which `tcfCryptoUtil` does not. To use `tcfCryptoUtil`, see the instructions in [Deploy the Custom Connector Toolkit](#), in the section "Create a Keystore for HTTPS Communication."

The following picture illustrates the A2A setup:

**Figure 29: A2A Keystore Password Encryption**



To set up A2A for securing the keystore password, complete the following tasks:

### Install the A2A Client

Install the A2A Client on the Custom Connector server and register the Client with PAM. For instructions, see [Install an A2A Client for Credential Management](#).

When you install the A2A Client, it sends a registration request to PAM. As part of the registration process, PAM creates a device, unless it finds an existing one. The device name is the fully qualified domain name or IP address of the host where the client is installed. The device type, which is set to A2A, is used later in this procedure.

**NOTE**

Edit the `cspmclient.xml` file, and remove the `preserveCacheBetweenRestarts` parameter. A2A Client does not need to cache credentials.

**Configure PAM Components for A2A**

Configure the following PAM components to secure the keystore with A2A:

- A2A device configuration
- Two password composition policies
- Two target applications, one for the keystore and one for both hash values
- Three target accounts, one for the key store, one for the call stack hash, and one for the file list hash
- An A2A script, which gets credentials from PAM
- An A2A target group (optional)
- A2A mappings for the target accounts

The following sections explain how to configure these components. The procedures list only the fields requiring configuration, including sample values. For step-by-step A2A configuration procedures, see [Add and Run Credential Manager A2A Requestors](#).

***Modify the A2A Device Configuration***

A device record is required for the appliance to establish a relationship between the Tomcat server and the A2A target accounts.

Select the A2A device for the registered A2A Client. For this procedure, assume that the A2A device has the following values:

- **Name:** `tcf.tomcat.host`  
Specify the host name of the Tomcat server where the TCF and A2A Client is installed.
- **Address:** `tcf.tomcat.host`  
The address field uses the same value as the Name field, whether the value is an IP address or a fully qualified domain name.

For the device to manage credentials for the keystore, add Password Management to the Device Type setting.

**Follow these steps:**

1. Go to **Devices, Manage Devices**.
2. From the list, select the A2A device record and select **Update**.
3. For the **Device Type** setting, select **Password Management**. The Device Type now is set to Password Management and A2A.
4. Select **OK** to save the changes.

***Create Two Password Composition Policies***

To specify the characteristics of the keystore password, the call stack and the file list hash values, configure two password composition policies. Create one policy for the keystore password. Create a second policy for the hash values.

Navigate to Credentials, Manage Targets, Password Composition Policies and configure the policies with the following values:

**Keystore Password Policy:** Configure a policy to generate a password for the keystore. The password for the keystore is kept only in memory, but make it a strong password of sufficient length.

- **Name:** Assign a descriptive name to the policy, such as KeyStorePCP.
- **Minimum Length** and **Maximum Length:** Set to 64 characters
- **Must Contain** and **First Must Contain:** Include uppercase, lowercase, and numeric characters. Avoid using special characters.

**Hashes Password Policy:** Configure a policy that defines the requirements for the call stack and file list hash values. The Custom Connector server calculates these hash values. Before the server requests the keystore password, it compares these hashes with the hashes that are stored in the target accounts at PAM.

- **Name:** Assign a descriptive name to the policy, such as TCFHashPCP.
- **Minimum Length** and **Maximum Length:** Set to 64 characters
- **Must Contain** and **First Must Contain:** Use only lowercase and numeric characters. Avoid using special characters.

### **Configure Two Target Applications**

Configure two target applications (Credentials, Manage Targets, Applications). One application is for the keystore password and one application is for the call stack and file list hash values.

**Keystore Target Application:** Specify the following values for the keystore application:

- **Host Name:** Enter the name of the A2A device (tcf.tomcat.host)
- **Device Name:** Enter the name of the A2A device (tcf.tomcat.host).
- **Application Name:** Enter a name to indicate that this target application is for the keystore (TCFKeyStoreApplication).
- **Application Type:** Generic
- **Password Composition Policy:** Specify the keystore password policy that you created (KeyStorePCP)

**Hashes Target Application:** Specify the following values for the hash values application:

- **Host Name:** Enter the name of the A2A device (tcf.tomcat.host)
- **Device Name:** Enter the name of the A2A device (tcf.tomcat.host).
- **Application Name:** Enter a name to indicate that this target application is for the hashes, such as TCFHashApplication.
- **Application Type:** Generic
- **Password Composition Policy:** Specify the hashes password policy that you created (TCFHashPCP).

### **Create Three Target Accounts**

Configure three target accounts—one for the keystore password, one for the file list hash and one for the call stack hash. The Custom Connector server calculates the hash values. You copy these values to the target accounts. Before the Custom Connector server requests the keystore password, it compares its calculated hashes with the target account hashes. The values must match.

**Keystore Target Account:** When you configure the keystore target account, you generate a password. This password gets encrypted and stored in the PAM database. Use this generated password for the keystore that you create at the Custom Connector server.

Specify the following values for the account and save the account:

- **Host Name:** Enter the name of the A2A device (tcf.tomcat.host)
- **Device Name:** Enter the name of the A2A device (tcf.tomcat.host).
- **Application Name:** Enter the name of the keystore target application (TCFKeyStoreApplication).
- **Account Name:** Enter a name indicating that this target account is for the keystore, such as TCFKeystore
- **Password View Policy:** Default
- **Account Type:** A2A Account
- **Aliases:** We recommend that you enter the same name as the target account name, TCFKeystore. You can specify a different value.
- **Cache Behavior:** No Cache
- **Password:** Select the key ring icon and generate a password.

In the Target Accounts list:

1. Select the keystore account that you created.
2. Under Action, select the eye icon to view the password.
3. Copy this password and save it. This value is required when you create a keystore at the Custom Connector server.

**Call Stack Hash Target Account:** Specify the following values for the account:

- **Host Name:** Enter the name of the A2A device (tcf.tomcat.host)
- **Device Name:** Enter the name of the A2A device (tcf.tomcat.host).
- **Application Name:** Enter the name of the target application you created for the hashes (TCFHashApplication).
- **Account Name:** Enter a name indicating that this target account is for the call stack hash, such as TCFCallStackHash.
- **Password View Policy:** Default
- **Account Type:** A2A Account
- **Aliases:** We recommend that you enter the same name as the target account name, TCFCallStackHash. You can specify a different value.
- **Cache Behavior:** No Cache
- **Password:** Select the key ring icon and generate a password. After the Custom Connector server generates the call stack hash, update this field with that hash value.

**File List Hash Target Account:** Specify the following values for the account:

- **Host Name:** Enter the name of the A2A device (tcf.tomcat.host)
- **Device Name:** Enter the name of the A2A device (tcf.tomcat.host).
- **Application Name:** Enter the name of the target application you created for the hashes (TCFHashApplication).
- **Account Name:** Enter a name indicating that this target account is for the file list hash, such as TCFFileListHash.
- **Password View Policy:** Default
- **Account Type:** A2A Account
- **Aliases:** We recommend that you enter the same name as the target account name, TCFFileListHash. You can specify a different value.
- **Cache Behavior:** No Cache
- **Password:** Select the key ring icon and generate a password. After the Custom Connector server generates the file list hash, update this field with that hash value.

### ***Identify the A2A Script that Retrieves the Keystore Password***

The A2A script, which is a Java class, runs on the Tomcat server. This script uses the A2A Client to fetch the keystore password from PAM. PAM calculates the script hash when one of the following requests occur:

- You select Get Script Hash when you add an A2A Script in the UI.
- The A2A Client uses the script to send a password request.



At PAM, identify the A2A script:

1. In the UI, select **Credentials, Manage A2A, Scripts**.
2. Select Add and specifying the following values:
  - **Client:** tcf.tomcat.host
  - **Device Name:** tcf.tomcat.host
  - **Script/App Name:** Enter the class name that calls the A2A Client. In this context, the class name is **com.ca.pam.extensions.tcfcryptoutil.TCFPropertySource**
  - **Execution Path:** Specify the directory where the Tomcat server is installed on Custom Connector server. Note: If the Execution Path check is enabled in the mapping, then paths that include soft links result in failure. Example: In the path /example/linkdir/test, if linkdir is a soft link to reldir, then the Execution Path should be /example/reldir/test.
  - **File Path:** Specify the location of the class. For example, the location is the /lib directory on the Tomcat server and the CryptoUtil JAR file name. For example: C:\DevTools\apache-tomcat-9.0.13\lib\capamextensionstcfCryptoUtil-4.16.0.jar
  - **Type:** Java
3. Select **OK**.

#### NOTE

The JAR file is determined by the version of the Tomcat server.

#### **Configure a Target and Request Group to Reduce A2A Mappings (Optional)**

PAM must authorize requesters who want to retrieve the keystore password. An A2A mapping is the mechanism that PAM uses to verify a request script and before releasing the requested credentials.

You can use a target group to organize the accounts for the keystore password, call stack hash, and file list hash. Using this target group requires only one A2A mapping. Without a target group, you have to configure individual mappings for each account. If several Custom Connector servers are deployed, use an A2A request group for A2A mappings.

#### **Create a Target Group**

A target group lets you organize target accounts. A target group can use filters on host servers, applications, and accounts. By using a target group for the keystore password and two hash target accounts, you can more easily manage authorization policies between clients and scripts.

#### **Follow these steps:**

1. From the UI, select **Credentials, Manage Targets, Target Groups**.
2. Add a group.
3. Complete the following settings:
  - **Name:** Enter a descriptive name, such as TCFTargetGroup
  - **Server** section: Select the Filter column for the Host Name. Filter on a string that is contained in the name of the Tomcat servers.
  - **Application** section: Select the Filter column for the **Application Name** field. Add a string that applies to all the relevant TCF target applications that you configured earlier. For example, for the Application Name, use this filter:



- **Account** section: Select the Filter column for the **Account Name** field. Add a string that applies to all the relevant TCF target accounts that you configured earlier.

#### **Create an A2A Request Group**

If you deploy two Custom Connector servers, a request group is useful. Both servers in the group need access to the keystore credentials.

**Follow these steps:**

1. From the UI, select **Credentials, Manage A2A, Request Groups**.
2. Add a group.
3. In the Client section, select the Filter column for the **Host Name** field. Filter on a string that is contained in the name of the Tomcat servers. Add a second host for the other Custom Connector server. Ensure both servers use the same A2A script.
4. In the Script section, select the Filter column for the **Name** field. Filter on the name of the A2A script you created previously. The following graphic shows how to configure the Script section of the A2A request group page:

Fields	Filters
<b>Client</b>	
Host Name	<a href="#">Not Specified</a>
Device Name	<a href="#">Not Specified</a>
IP Address	<a href="#">Not Specified</a>
Descriptor 1	<a href="#">Not Specified</a>
Descriptor 2	<a href="#">Not Specified</a>
<b>Script</b>	
Name	<b>WHERE</b> Script.Name <a href="#">beginswith 'com.ca.pam.extensions.tfcryptout</a>

5. Continue to the next section and create an A2A mapping.

**Create an A2A Mapping for Requester Authorizations**

The final configuration step at PAM is to configure an A2A mapping for requester authorizations. Create a mapping between the A2A script running on the Tomcat server and the individual target account or A2A target group. This mapping tells the appliance to authorize the A2A script, the requester, and grant access to credentials.

A mapping to a target group includes aliases for all accounts in the group. A mapping from a request group includes all Custom Connector servers in the group.

If your environment has only one Custom Connector server, add an A2A authorization mapping for a single client.

To map the script to a single Tomcat server, specify the following values:

- **Target:** Select **Group** and specify the TCFTargetGroup
- **Request:** Select **Client** and enter the IP address of the A2A Client
- **Script:** Select **Individual** and specify the name of the script, com.ca.pam.extensions.tfcryptoutil.TCFPropertySource
- **Check Execution User/Execution User:** Select this checkbox and specify the user administering the Tomcat server.
- **Check Execution Path:** Select this checkbox
- **Check File Path:** Select this checkbox
- **Perform Script Integrity Validation:** Select this checkbox

To map the script to multiple Tomcat servers, specify the following values:

- **Target:** Select **Group** and specify the Tomcat keystore
- **Request:** Select **Group** and select the name of the request group you created previously.
- **Check Execution User/Execution User:** Select this checkbox and specify the user administering the Tomcat server.
- **Check Execution Path:** Select this checkbox
- **Check File Path:** Select this checkbox
- **Perform Script Integrity Validation:** Select this checkbox

### **Configure the Custom Connector to Obtain the Keystore Password**

After you set up the A2A components at PAM, set up the Custom Connector server to retrieve the keystore password. Some of the appliance configuration settings are required to create and secure the keystore.

#### ***Create a Keystore and Encrypt the Keystore Password***

To secure communication between PAM and the Custom Connector, create a PKCS12 keystore. The keystore must contain an X.509 private key and certificate pair in PEM format. When you generate the keystore, the keystore password is in plain text. Encrypt the password using a TCF-provided utility, configTCF.

#### **NOTE**

The keystore that holds the X.509 key/certificate pair is separate from the keystore to secure the payload from PAM.

#### **Example: Keystore Set Up Using Keytool**

Many tools are available to create a keystore. The following procedure uses the keytool utility as an example.

#### **TIP**

The keys expire after the number of days that are specified by the `-validity` command argument. In the following procedure, the keys expire after 360 days. To regenerate the keys after they expire, repeat this procedure.

#### **Follow these steps to create a keystore and encrypt the password:**

1. Create a PKCS12 keystore by entering the following keytool command. If you created a keystore when you initially deployed the Custom Connector, do not create a new one. Move on to step 2.

```
keytool -genkey -alias pam -keyalg RSA -keysize 2048 -storetype PKCS12 -dname
"CN=capamtcf, OU=PAM, O=CA, L=Burlington, ST=MA, C=US" -keypass password-
storepass password -keystore <keystore_file> -validity 360
```

*password* is the password that you assigned when you created the [keystore target account](#).

*keystore\_file* is path and file name where you want to generate the keystore

This command output is an encrypted keystore password that is displayed on the command prompt.

2. Continue to the next procedure.

#### ***Add the Keystore Location to the server.xml File***

Specify the location of the keystore:

1. Edit the server.xml file in %CATALINA\_HOME%\conf\.
2. Locate the connector for HTTPS scheme
3. Add the following lines:

```
<Connector
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  port="8443" maxThreads="200"
  scheme="https" secure="true" SSLEnabled="true"
```

```
keystoreFile="keystore_file" keystorePass="${tomcat.keystore.pwd}"
clientAuth="false" sslProtocol="TLS"/>
```

*keystore\_file* is the file path and name of the PKCS12 keystore you created previously.

4. Continue to the next section.

### **Enable Tomcat to Read the TCF Properties**

Modify the catalina.properties file to enable Tomcat to read the TCF properties:

#### **Follow these steps:**

1. Navigate to the file %CATALINA\_HOME%\conf\catalina.properties .
2. Edit the file by adding the following lines to the end of it:

```
org.apache.tomcat.util.digester.PROPERTY_SOURCE=com.ca.pam.extensions.tcfcryptoutil.TCFProperties
tomcat.keystore.pwd.usea2a=true
tomcat.keystore.pwd=TCFKeyStore
tomcat.callstack.hash.alias=TCFCallStackHash
tomcat.file.list.hash.alias=TCFFileListHash
```

The entries provide the following information:

- The line beginning `org.apache.tomcat` : Overrides the default behavior to read the properties.
- `tomcat.keystore.pwd.usea2a=true`: Instructs Tomcat to retrieve the keystore password from PAM. With this set to true, the following lines are required:
  - `tomcat.keystore.pwd=TCFKeyStore` : Alias for the keystore password target account that is stored at PAM.
  - `tomcat.callstack.hash.alias=TCFCallStackHash` : Alias for the call stack hash target account
  - `tomcat.file.list.hash.alias=TCFFileListHash` : Alias for the file list hash target account

### **Enable the Custom Connector Server to Retrieve Credentials**

For the Custom Connector server to retrieve credentials from PAM, add the A2A Client API libraries and TCF libraries to its class paths.

In the following procedure:

- The directory paths and place holders reflect a UNIX/LINUX system. Windows paths use backward slashes and placeholders use % signs.
- `cspmclient/lib` is located under `CSPM_CLIENT_HOME`, the installed location of the A2A Client on your system
- `CATALINA_HOME` is the installed location of the Tomcat server

#### **Follow these steps:**

1. Copy the following A2A JAR files from `CSPM_CLIENT_HOME/cspmclient/lib` to `$CATALINA_HOME/lib`
  - `cspmclient.jar`
  - `cwjcafips.jar`
2. Copy the appropriate A2A Client libraries for your platform:
  - UNIX/Linux platforms:
    - a. Copy the following libraries from `$CSPM_CLIENT_HOME/cspmclient/lib` to `$CATALINA_HOME/lib`
      - `libcpaspiffadaptor64.so`
      - `libcspminterface64.so`
      - `libcwjcafips.so`
    - b. For Tomcat to recognize these libraries, set the `LD_LIBRARY` path in the `setenv.sh` script. This script is located in `$CATALINA_HOME/bin/`.  
 Example path: `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/$CATALINA_HOME/lib`
  - Windows platforms: copy the following DLL files from `%CSPM_CLIENT_HOME%\cspmclient\lib` to `%CATALINA_HOME%\bin`:

- • cpaspiffadaptor64.dll
  - cspminterface64.dll
  - cwjcafips.dll
3. Copy the capamextensionstcfCryptoUtil-4.16.0.jar file from `TCF_HOME/configTCF` to `$CATALINA_HOME/lib`. `TCF_HOME` is where you extracted the Custom Connector Framework zip file.

### Create a File List for Verifying Deployed Files

Before the Custom Connector server fetches the keystore password, it verifies the integrity of its files. The Custom Connector server adds all the file hashes together and calculates one consolidated hash value of its files. The server compares this hash with the hash of the file list target account, which is retrieved from PAM. The hash values must match.

To generate the hash, the server needs a list of all the deployed target connector files.

#### Follow these steps:

1. Create a file and name it **pam.filelist**. This name is the required file name.
2. In the pam.filelist file, include the:
  - full path of the pam.filelist file itself
  - full path of the capamef.war file
  - full path for all the files that are extracted from the .war files in the **webapps** and **webapps\_targetconnectors** folders
  - full path of all custom target connectors that are deployed on the Custom Connector server.
  - Optionally, the full path of libraries in the **lib** directory under `%CATALINA_HOME%`

All paths and file names are case-sensitive.
3. Save the file.
4. Copy the file to `%CATALINA_HOME%\conf`.
5. Restart the Tomcat server.

The following example is a simple file list. An actual file list contains more files, such as the files extracted from the .war files in the **webapps** and **webapps\_targetconnectors** folders.

```
C:\DevTools\apache-tomcat-9.0.13\conf\pam.filelist
C:\DevTools\apache-tomcat-9.0.13\webapps\capamef.war
C:\DevTools\apache-tomcat-9.0.13\webapps_targetconnectors\exampleTargetConnector.war
C:\DevTools\apache-tomcat-9.0.13\webapps_targetconnectors\echoTargetConnector.war
```

### Copy the Hash Values to Target Accounts

When the Custom Connector requests the keystore password, it calculates the call stack and file list hash values. The server then compares these values to the target account hashes. The values must match before PAM responds with the keystore password.

For the hashes to match, you must copy the calculated values to the target accounts at PAM.

#### To compare hashes, follow these steps:

1. Start the Custom Connector server but expect startup to fail.  
At startup, the server calls PAM and fetches the hash values. Startup fails because the hashes obtained from PAM do not match the values that are calculated by the Custom Connector server.
2. Open the catalina.log file in `%CATALINA_HOME%\logs` directory.
3. Look for the following two messages in the log file:
 

```
Computed callstack hash: callstack_hash does not match the retrieved call stack
hash: CA_PAM_call_stack_hash
```

Computed filelist hash: *filelist\_hash* does not match the retrieved filelist hash: *CA\_PAM\_file\_list\_hash*

4. Copy the hashes from these log messages and paste them into the **Password** tab of the associated target accounts at PAM.
  - *callstack\_hash*: The computed value from the call stack target account
  - *filelist\_hash*: The computed value from the file list target account
5. Restart the server.

When the Custom Connector server restarts, it requests the hashes from PAM, which are verified successfully. Finally, the Custom Connector server retrieves the keystore password from PAM.

## Troubleshooting

If exceptions are logged during startup of the Tomcat server, look at the catalina log file. If the exception stack trace looks like the following graphic, the server cannot start the HTTPS connector.

```
01-Nov-2018 14:59:46.063 INFO [main] org.apache.coyote.AbstractProtocol.init
  Initializing ProtocolHandler ["https-openssl-nio-8443"]
01-Nov-2018 14:59:46.401 SEVERE [main]
  org.apache.catalina.util.LifecycleBase.handleSubClassException Failed to initialize
  component [Connector[HTTP/1.1-8443]]
org.apache.catalina.LifecycleException: Protocol handler initialization failed
at org.apache.catalina.connector.Connector.initInternal(Connector.java:935)
at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:136)
at org.apache.catalina.core.StandardService.initInternal(StandardService.java:533)
at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:136)
at org.apache.catalina.core.StandardServer.initInternal(StandardServer.java:852)
```

The reasons for this problem are:

**Problem:** The keystore password is incorrect.

The password is retrieved from PAM, but it is incorrect. Verify the retrieval by checking the catalina.log for the message:

A2A Client Status Code: 400

Examine the following stack trace in the catalina.log file:

```
Caused by: java.io.IOException: keystore password was incorrect
at sun.security.pkcs12.PKCS12KeyStore.engineLoad(PKCS12KeyStore.java:2015)
at sun.security.provider.KeyStoreDelegator.engineLoad(KeyStoreDelegator.java:238)
at sun.security.provider.JavaKeyStore$DualFormatJKS.engineLoad(JavaKeyStore.java:70)
at java.security.KeyStore.load(KeyStore.java:1445)
at org.apache.tomcat.util.net.SSLUtilBase.getStore(SSLUtilBase.java:179)
at
  org.apache.tomcat.util.net.SSLHostConfigCertificate.getCertificateKeystore(SSLHostConfigCertificate.java:144)
at org.apache.tomcat.util.net.jsse.JSSEUtil.getKeyManagers(JSSEUtil.java:203)
```

**Solution:** In the PAM UI, verify that the password in keystore target account is correct. Also, verify that the Tomcat keystore has the same password.

**Problem:** The A2A Client is not started. The catalina.log file contains the message: A2A Client Status Code: 402

**Solution:** Start the A2A client daemon (UNIX)/service (Windows).

**Problem:** The keystore password alias in the catalina.properties file is not found in PAM. The catalina.log shows the message: `A2A Client Status Code: 405` **Solution:** In the PAM UI, look at the name of the keystore target account. At the Tomcat server, look at the catalina.properties file. Confirm that the `tomcat.keystore.pwd.alias` property has the same name as the target account.

#### NOTE

If the call stack or filelist hash alias is not found in PAM, the error and solution are the similar. Look in the UI and the catalina.properties file and ensure that the aliases match.

**Problem:** Unauthorized Script Name. The A2A mapping uses an incorrect script name. The catalina.log contains the message: `A2A Client Status Code: 409` **Solution:** Fix the A2A script to match the mapping and script program.

**Problem:** Unauthorized execution path. The A2A mapping does not have the correct execution path for the script. The catalina.log contains the message: `A2A Client Status Code: 410`

**Solution:** Verify the execution path. In the PAM UI, navigate to **Credentials, Reports, Activities**. Select **Configure** to set up the activities report. Add an entry using the **+** sign then select the **Failed A2A Client Requests in Last 30 days** item. After the report runs, look for the entry with the 410 error code. That entry includes the execution path for the A2A client request. Specify this execution path in the A2A script.

**Problem:** Unauthorized execution user. The A2A mapping does not specify the correct user. The catalina.log includes the message: `A2A Client Status Code: 411` **Solution:** Change A2A mapping to use the same user that is running the Tomcat server.

**Problem:** Incorrect script hash value. The hash value of the Custom Connector Java class file is incorrect or the wrong script is specified. The catalina.log includes the message: `A2A Client Status Code: 436`

**Solution:** If the Custom Connector Java class file is changed intentionally, recalculate the hash. Select the **Get Script Hash** button on the script panel PAM UI.

## Try Out the Sample Custom Connectors

To help you develop your own connectors, the Custom Connector software comes with two sample target connectors:

- **Echo target connector (echoTargetConnector.war)** – This sample connector displays the requests that are sent from the appliance to the TCF. Use this sample to verify the UI definitions and the data flow for the connector.
- **Example target connector (exampleTargetConnector.war)** – This sample lets you view and update passwords on a Linux target device.

The .war files for these sample connectors are in the **samples** folder.

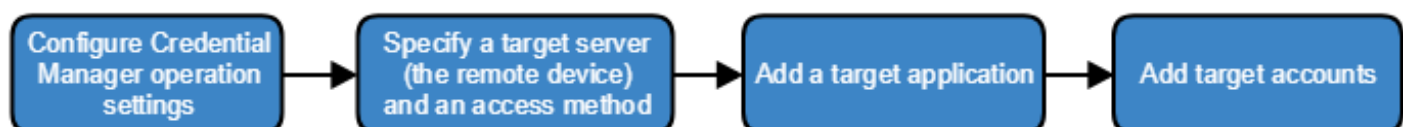
Use one or both of them to help you understand how custom target connectors work.

#### WARNING

Do not use the Example Target Connector in a production environment.

The steps for configuring a custom target connector are no different from the out-of-the-box connectors. When trying out the sample connectors, follow this procedure, which is shown in the following graphic:

**Figure 30: Credential Manager target configuration tasks**





**NOTE**

In a typical production environment, an access policy is configured. This policy lets a user or administrator to view and update credentials from the Access page in the UI. To test the sample target connectors, these procedures use an alternative method. You view and update credentials from the target account page.

**Use the Echo Target Connector to Follow Requests to the TCF**

The Echo Target Connector demonstrates the requests that are sent from the appliance to the TCF. Information from the Echo Target Connector connector is echoed to the catalina.out log file on the Custom Connector server. By examining the log, you can see all of the available UI fields and controls from the uiDefinitions.json file. You can also see the information that the target connector extracts from the payload that is sent by the TCF.

Complete the following procedures to configure the Echo Target Connector and view the catalina.out file on your Custom Connector server:

1. Specify a remote target server.
2. In the UI, add the Echo Target Connector application
3. Add an account to the echo target connector application
4. Update the password and view the catalina.out log file.

Each procedure is explained in the next sections.

***Specify a Remote Target Server***

You do not need an actual target server when using the echo target connector. This connector only tests communication between the appliance and the TCF. However, you must specify a target server, even a fake entry, for the configuration in the UI.

**Follow these steps:**

1. Log in the Privileged Access Manager UI.
2. In the UI, select **Devices, Manages Devices**.
3. From the Devices page, select **Add**.
4. In the Add Device dialog, complete the required fields in the Basic Info tab.
5. For the **Device Type**, select the **Password Management** checkbox. Keep the Access checkbox selected.
6. Go to the **Access Methods** tab and specify an access protocol, such as SSH. The appliance uses the access method to contact the remote target server.
7. Select **OK** to complete the configuration.

Now, add the target application as instructed in the next procedure.

***Add the Echo Target Connector Application***

Configure the Echo Target Connector application.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Select or enter values for the following fields:
  - Host Name: Select the magnifying glass to pick the target server you defined in the previous procedure.
  - Device Name: Enter the name for the target server you added.
  - Application Name: Specify an application name, such as echoapp. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Echo Target Connector**.  
A new tab labeled **Echo - Application** displays.



5. On the **Echo - Application** tab, change the default settings on this page. If you change the settings, you can see the new values in the Tomcat catalina.out file when you validate the credentials.
6. Select **OK**.

Continue on and add a target account for the echo target application.

### **Add the Target Account**

Add a target account that you want to associate with the target application. When you configure a target account, identify a target application for that account. Target account user names must be unique for a given target application.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. Complete the following fields:
  - **Host Name:** Enter the IP address of the remote target server you defined.
  - **Device Name:** Enter the name for the target server.
  - **Application Name:** Select the Echo Target Application name that you configured in the previous procedure.
  - **Account Name:** Assign a unique account name for a given target application. The Echo Target Connector does not connect to a target server, so you can enter any name. Suggestion: echo
  - **Password View Policy:** Accept the default password view policy.
  - **Protocol:** This field is filled-in automatically after you specify a device.
  - **Password:** The password of the user account at the remote target server. For testing the Echo Target Connector, we recommend that you select the Generate Credential icon (keys on a ring).  
The generated password follows the password composition policy, and it updates automatically at the target server.
  - **Account Type:** Accept the default, Privileged Account.
4. Select **OK** to save the account.
5. Keep the account page open and go to the next procedure.

### **Update Credentials and Examine the Log File**

1. From the account page you created, select the Generate Credential icon (keys on the ring) and generate a new password.
2. Select **OK** to save the new password.
3. Select the Verify Credential icon (person with a green checkmark) and select **OK**.
4. Log in to the Tomcat system where you deployed the TCF.
5. Open the catalina.out file and look for the contents of the REST web service. Review the entries for the updated credential.

The log file entries illustrate the exchanges between the appliance and the TCF. The file also includes the UI definitions that render the Echo Target Connector application and account tabs in the UI.

### **Use the Example Target Connector to View and Update a Password**

The Example Target Connector demonstrates an end-to-end communication flow. Beginning at the appliance, the connector shows the request to the TCF, through to the target connector, and ending at the remote target server.

#### **WARNING**

Do not use the Example Target Connector in a production environment.

Before you can use the Example Target Connector:

- Complete the prerequisites
- Install an SSH Utility on the Custom Connector Server
- Follow the procedures to configure the target server, target application, and target account on the appliance.

After you complete these tasks, try viewing and updating a password.

### **Prerequisites**

- Set up a remote Linux target server
- Set up a user account whose password you can change.  
Verify that you can log in to the Linux system as that user. Use SSH to connect to the Linux system. If the user can log in, the Example Target Connector can communicate to the target.

### **Install an SSH Utility on the Custom Connector Server**

The Example Target Connector lets you verify and update passwords on a UNIX target device. To use the Example Target Connector, install the utility on the Custom Connector server where the TCF is installed:

- [Install the sshpass utility \(UNIX\)](#)
- [Install PuTTY Link \(Plink\) \(Windows\)](#)

#### **NOTE**

You can install the Custom Connector server on a UNIX or Windows system. However, the Example Target Connector is for use only with a UNIX target device.

You do not have to execute any commands with these utilities. The example target connector executes commands automatically.

#### **Install sshpass on the UNIX System Running Tomcat**

If the Custom Connector server is running on a UNIX platform, install the **sshpas** utility. The sshpass utility lets you run keyboard interactive authentication in non-interactive mode. The command to install sshpass differs depending on the type of UNIX system you are using.

Installation command examples:

- On a Linux system, enter the following command:

```
$ sudo yum install sshpass
```

- On a Debian/Ubuntu system, enter the following command:

```
$ sudo apt-get install sshpass
```

#### **Install the PuTTY Link Utility on the Windows System Running Tomcat**

If the Custom Connector server is running on a Windows system, download and install the PuTTY SSH client. The client includes the Plink utility, which you can use to run non-interactive SSH sessions. The Example Target Connector uses Plink.

### **Specify the Remote Linux Target Server**

Add the Linux target server as a target device.

#### **Follow these steps:**

1. Log in the Privileged Access Manager UI.
2. In the UI, select **Devices, Manages Devices**.

3. From the Devices page, select **Add**.
4. In the Add Device dialog, complete the required fields in the **Basic Info** tab.
5. For the **Device Type**, select the **Password Management** checkbox. Keep the Access checkbox selected.
6. Go to the Access Methods tab and specify an access protocol, such as SSH. The appliance uses the access method to contact the remote target server.
7. Select **OK** to complete the configuration.

Now, add the Example Target Application.

### ***Add the Example Target Connector Application***

Configure the Example Target Connector application.

#### **Follow these steps in the UI:**

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add**.
3. Complete the following fields:
  - Host Name: Select the magnifying glass to pick the target server.
  - Device Name: Enter the name for the Linux target server.
  - Application Name: Specify an application name, such as exampleapp. Application names must be unique for a given target server.
4. In the **Application Type** field, select **Example Target Connector**.  
A new tab labeled **Example - Application** displays.
5. On the Example - Application tab, we recommend that you change the settings. If you change the settings, you can see the new values in the Tomcat catalina.out file when you validate the credentials.
6. Select **OK**.

Now add the example target account.

### ***Add the Example Target Account***

Add the Linux user account as a target account. Target account user names must be unique for a given target application.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. Complete the following fields:
  - **Host Name:** Select the remote Linux system from the drop-down list.
  - **Device Name:** Enter the name of the remote Linux system.
  - **Application Name:** Select the example application that you configured in the previous procedure. An **Example - Account** tab displays. On this tab, optionally add an account description and select a master account with privileges to log in on behalf of the user.
  - **Account Name:** Assign a unique account name for a given target application. The account name that you enter must match the account name that is used by the target system. For example, on a Linux system, account names are the user ID (userid).
  - **Password View Policy:** Use the default password view policy.
  - **Protocol:** This field is filled-in automatically after you specify a device.
  - **Password:** For this example, we recommend that you select the Generate Password icon (keys on a ring). The generated password follows the password composition policy, and it updates automatically at the target server.
  - **Account Type:** Accept the default, Privileged Account.
4. Select **OK** to save the account.
5. Keep the account page open and go to the next procedure.

## View and Update the Password

After you specify the Example - Application and the target account, you can verify and change the password.

### Follow these steps:

1. Select the target account and then select Update.
2. Select the **Password** tab.
3. Select the option **Update both the Credential Manager System and the target server**.
4. Select **OK**.  
The appliance verifies the password at the target system. If the verification is successful, a green checkmark is placed in the Verified column for the target account entry.
5. Select the target account entry again and select Update.
6. View the current password by selecting the View Credential icon (the eye) next to the **Password** field.
7. Select the **Generate Password** icon (keys on a ring).
8. Select **OK**. The password is updated.
9. Select the **Verify Credential** icon (person with a green checkmark) the select **OK**.  
After successful verification, view the password again to see that it has changed.

### NOTE

Continue by reading [Learn How to Use the Custom Connector Components](#). Review this information carefully before building your own target connector.

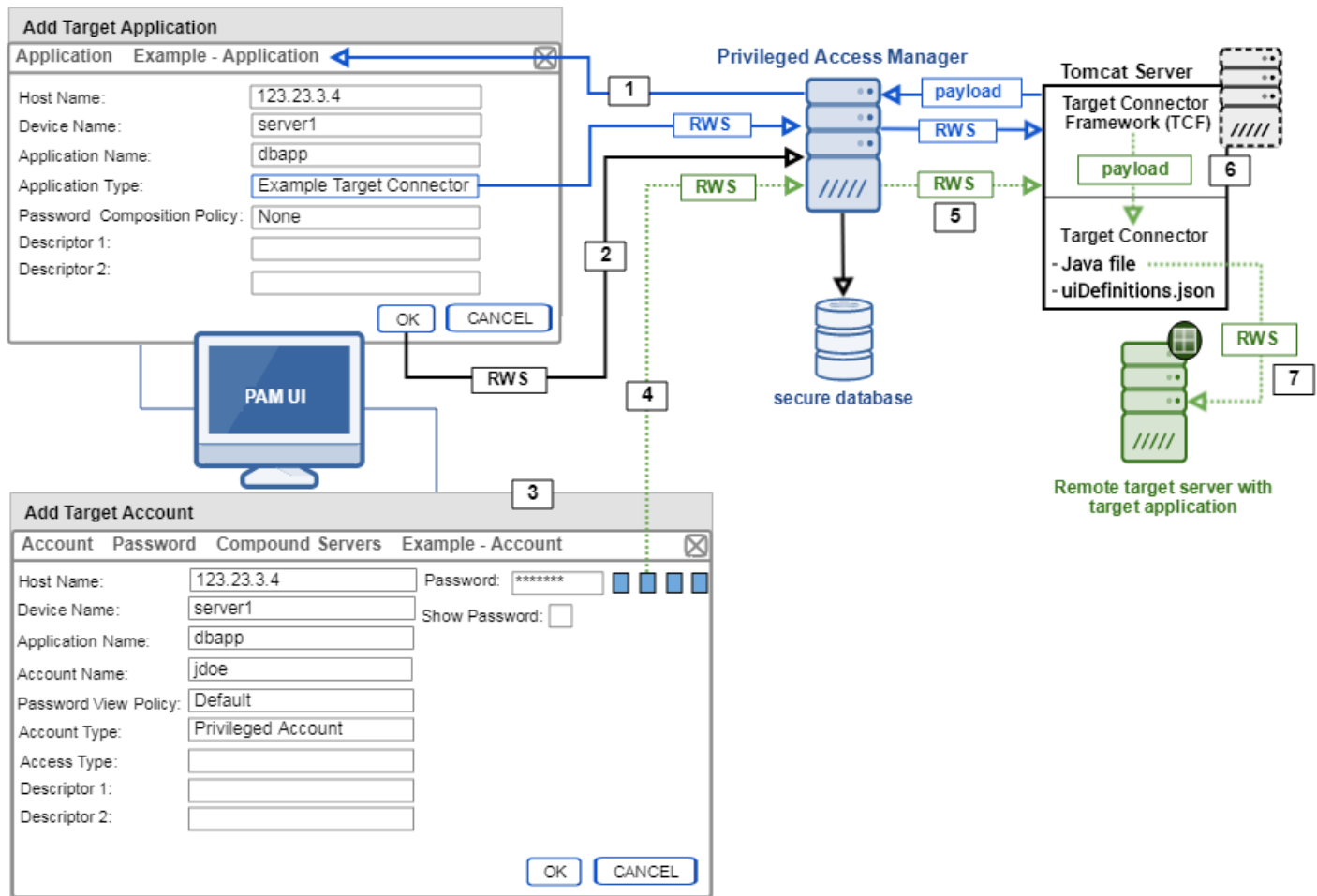
## Learn How to Use the Custom Connector Components

Before you build your own custom target connectors, familiarize yourself with the major components and how these components are used at runtime.

A custom target connector uses the following components to work with the TCF:

- **uiDefinitions.json file** –This JSON file includes the custom target connector fields that are displayed in the UI. This file also determines the attributes that are saved in the appliance database. To customize the UI for your applications and accounts, you define attributes in the uiDefinitions.json file.
- **REST web service endpoints (RWS)** – The Java code that you write for the custom target connector must support three REST web service endpoints: UI definitions, validations, and credentials. Each service provides a unique function for the TCF and target connector operation.

The following diagram illustrates how the appliance and the TCF use the uiDefinitions.json file and the Java code at runtime:

**Figure 31: Runtime flow of a TCF Transmission**

After a custom target connector is deployed, the custom application type and account are available in the UI.

When an administrator adds a target application and selects a custom application type, such as Example Target Application the following runtime sequence occurs:

1. The appliance contacts the TCF, which returns a JSON payload to the appliance and the UI. The tab for the custom application is rendered.
2. The administrator completes the settings on the custom application tab and selects **OK** to save this entry. The UI makes a REST web service call to the appliance.
3. The appliance stores the attributes that are sent from the UI in its database.
4. The administrator adds a target account that is associated with the custom application type.
5. When the View Password icon or the Validate Credential icon on the account page is selected, the UI sends another REST call to the appliance.
6. The appliance recognizes the call as a request for an external resource, and sends a REST call to the TCF.
7. The TCF sends a REST call with a payload to the target connector to complete the view or validate credential request. The payload is determined by the attributes in the uiDefinitions.json file. The Java code parses the payload and extracts the data that it needs. The Java code uses the "field" attribute of each entry in the JSON file to identify and extract the necessary data.
8. The target connector now has access to the application on the target server.

To learn about the `uiDefinitions.json` and the web service endpoints in detail, go to the following topics:

- [UI Fields and Controls for Configuring Connectors](#)
- [Web Service Endpoints for the Custom Connector](#)

After you are familiar with these two components, you can edit them when you go to [build your own custom connectors](#).

## UI Fields and Controls for Configuring Connectors

The PAM UI must be able to render the tabs and input controls for the target application and account. The UI fields and controls are defined in a JSON file named **uiDefinitions.json**. When an administrator selects a custom connector, the appliance contacts the TCF. The TCF then returns the JSON payload to the appliance and the UI. The UI displays the tabs and settings that are defined in the JSON file.

This topic provides reference information that describes the `uiDefinitions.json` file. The contents of this file determines how UI panels and controls for your custom target connector are displayed. When you are ready to build a custom target connector, modify the `uiDefinitions.json` file and then validate your changes with the UI validator utility. These tasks are explained in the topic [Build Your Custom Connector](#).

### Structure of the uiDefinitions.json File

The `uiDefinitions.json` file is organized into three main sections:

- **account** – specifies the target account at the appliance  
A single "account" attribute definition that contains a single child "uiDefinition" attribute are required.
- **application**– specifies the target application at the applianceA single "application" attribute definition that contains a single child "uiDefinition" attribute are required.
- **locale** – specifies the language of the field labels when the UI controls are shown in different languages. See [Define the Locale for UI Field Labels](#) later in this topic.

### **Account and Applications Sections**

The account and applications sections can include one or more tabbed panels. Each panel can contain groups of related target application or target account attributes. For example, the `uiDefinitions.json` file for the Example Target Connector contains an "application" section. This section defines a panel with an **Example - Application** tab and a series of fields that define the UI controls. The controls identify details about the connector. The JSON file also has an "account" section with a tab **Example - Account**, a description field and a target account drop-down list.

#### **WARNING**

The JSON file must include an "account" and "application" section.

The following two panels are rendered by the `uiDefinitions.json` file that follows the panels.

## Add Target Account



Account Password Compound Servers Example - Account

Description:

Master Account:

OK

CANCEL

## Update exampleapp

Application Example - Application

Connect Timeout: 60000

Read Timeout: 5000

SSH Port: 22

Connector Protocol: ☐ SSL ☐ TLS 1.0 ☒ TLS 2.0

Additional Encryption: AES

Use Certificate: ☐

Certificate:

```

{
  "account": {
    "uiDefinition": {
      "tabs": [{
        "id": "ExampleAccDetail",
        "label": "Example - Account",
        "fields": [{
          "type": "TEXT",
          "field": "description",
          "label": "Description",
          "maxLength": 60
        }, {
          "type": "TARGETACCOUNT",
          "field": "anotherAccount",
          "label": "Master Account"
        }]
      }]
    }
  },
  "application": {
    "uiDefinition": {
      "tabs": [{
        "id": "ExampleAppDetail",
        "label": "Example - Application",
        "fields": [{
          "type": "NUMBER",
          "field": "connectTimeout",
          "label": "Connect Timeout",
          "minValue": 1,
          "value": 60000
        }, {
          "type": "NUMBER",
          "field": "readTimeout",
          "label": "Read Timeout",
          "minValue": 1,
          "value": 5000
        }, {
          "type": "NUMBER",
          "field": "sshPort",
          "label": "SSH Port",
          "minValue": 0,
          "maxValue": 65535,
          "value": 22
        }, {

```



```

        "type": "RADIO",
        "field": "connector_protocol",
        "label": "Connector Protocol",
        "value": "TLS_1.2",
        "values": [{
            "label": "TLS 1.0",
            "value": "TLS_1"
        }, {
            "label": "TLS 1.2",
            "value": "TLS_1.2"
        }, {
            "label": "TLS 1.3",
            "value": "TLS_1.3"
        }]
    }, {
        "type": "COMBOBOX",
        "field": "additionalEncryption",
        "label": "Additional Encryption",
        "value": "AES",
        "values": [{
            "label": "Triple DES",
            "value": "TRIPLEDES"
        }, {
            "label": "RSA",
            "value": "RSA"
        }, {
            "label": "Blowfish",
            "value": "BLOWFISH"
        }, {
            "label": "Twofish",
            "value": "TWOFISH"
        }, {
            "label": "AES",
            "value": "AES"
        }]
    }, {
        "type": "CHECKBOX",
        "field": "useCertificate",
        "label": "Use Certificate",
        "value": false
    }, {
        "type": "TEXTAREA",
        "field": "certificate",
        "label": "Certificate"
    }]
}]

```

```

    }

}

}

```

## How the Web Service Java Code Uses the UI Definitions

The "account" and "application" sections of the uiDefinitions.json file have a "uiDefinitions" attribute with a single "tabs" attribute. The tabs attribute allows you to define high-level tabs to group related fields together. Each tab contains a "fields" section, which defines all the individual configurable settings and controls for all connector-relevant data. Under the "fields" section are the individual connector-specific attributes, one of which is named "field".

The "field" attribute is used in the following ways:

- Each field serves as a unique identifier that allows the TCF to access data values.
- For all field attributes in the uiDefinitions.json file, validation of field values occurs automatically based on the definitions file. To execute any custom validation, such as cross-field validation for fields dependent on one another, you must add validation logic to the **Validations.java** file. In the topic [Build Your Custom Connector](#), see the section, "Edit Web Service Endpoints" for instructions about adding validation logic.
- If you remove a field from the uiDefinitions.json file, edit your Java code so it no longer references the field. This instruction applies to the Credentials.java file and the Validations.java file.
- All field values are defined as strings in the JSON payload. You might need to do some data type conversions in your Java code.

The remainder of this topic describes the different attributes and constraints for each field type.

## UI Tabs and Controls for Target Applications and Accounts

The following table describes the characteristics of the UI tabs and controls for the custom target connector-specific settings that you see in PAM UI. Specific details for each type are described later in this topic.

Attribute	Description
type	<p>(Required) Identifies the kind of field and the type of data value entry and validation options are allowed.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• TEXT – plain text entries for fields like user names</li> <li>• TEXTAREA – displays a block of text, such as a certificate</li> <li>• NUMBER – for integer data, such as port numbers</li> <li>• PASSWORD – for passwords that are entered in plain text that are masked in the UI.</li> <li>• CHECKBOX – provides a selectable box next to each option so a user can make a binary true or false choice.</li> <li>• COMBOBOX – provides a drop-down list for selecting only one of a predefined set of mutually exclusive options</li> <li>• RADIO – provides a radio button for selecting only one of a predefined set of mutually exclusive options</li> <li>• TARGETACCOUNT – provides a drop-down list of configured target accounts from which to select an account.</li> </ul>

field	(Required) Unique identifier for referencing the field and accessing data values. Identifiers must be unique for the defined target application or account. Every identifier must begin with a letter or underscore, followed by one or more letters, underscores or digits. You can follow an initial underscore with another underscore. Valid entries for this attribute are case-sensitive. A field value cannot contain embedded spaces.
label	(Required) Labels the control, such as the field name, the radio button label, or the checkbox label. If the value of the label is an identifier from the "locale" section of the file, the language-specific string is used. If a locale identifier is not specified, the literal string value is used. For more details, see <a href="#">Define the Locale for UI Field Labels</a> later in this topic.
value	(Optional) Designates the initial default value for new records.
values	(Required) An array of objects which contain a label and a value. This attribute is used by the RADIO and COMBOBOX attribute types.

### Constraints for Specific Field Types

For many of the attribute types, you can specify certain constraints for the field values. Pattern constraints let you require and restrict what values can be entered by the user. If the value provided does not meet the constraints, the UI displays a message with the valid entry criteria.

The following table lists the constraints that are allowed in the uiDefinitions.json file:

Constraint	Description	Used by Field Type
required	(Optional) Specifies whether a field value must be provided. A red asterisk displays next to the field label, indicating the field required. Valid entries: <ul style="list-style-type: none"> <li>false (default value). The field value is not required</li> <li>true. The field value is required for basic field validation</li> </ul>	TEXT, TEXTAREA, PASSWORD, NUMBER, TARGETACCOUNT
maxLength	(Optional) Maximum length for the field value	TEXT, TEXTAREA, PASSWORD
minLength	(Optional) Minimum length for the field value	TEXT, TEXTAREA, PASSWORD
minValue	(Optional) Minimum field value allowed	NUMBER
maxValue	(Optional) Maximum field value allowed	NUMBER
patternConstraint	(Optional) Specifies a regular expression that the connector tests against the field value during validation. If the test fails, the UI marks the field invalid when the user enters or saves the invalid entry.	TEXT, TEXTAREA, PASSWORD

patternConstraintMessage	(Optional) Contains the error message that the connector displays when a patternConstraint is used and the validation test fails. By default, this attribute is set to: "The value in this field is invalid"	TEXT, TEXTAREA, PASSWORD
--------------------------	---	--------------------------

### Examples of pattern constraints:

```
"patternConstraint": "^(today|tomorrow|yesterday)$"
"patternConstraintMessage": "Enter today, tomorrow or yesterday"
"patternConstraint": "^(?: (25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1[0-9][0-9]|1[0-9][0-9]|1[0-9][0-9]) (\. (?!$) |$) ) {4}$"
"patternConstraintMessage": "Enter a valid IPV4 address 12.22.111.132"
"patternConstraint" = "^\\((?([0-9]{3})\\)?[-. ]?(?([0-9]{3})[-. ]?(?([0-9]{4}))$";
"patternConstraintMessage" = 'Enter a valid phone number 555-555-5555 or (555)555-5555';
"patternConstraint": "^(5[0-9]{3,4}|[1-4]\\d{3,4}|[6-9]\\d{3})?$"
"patternConstraintMessage": - "Enter integer in the range [5000..59999]"
```

To see pattern constraint examples within a JSON file, go to [Create a TEXT, TEXTAREA, and PASSWORD Attributes](#).

### Review UI Definitions using an Example JSON File

To show how the UI definitions render the UI panels, examine the JSON file for the Example Target Connector. One "application" section and one "account" section are in the file.

#### NOTE

To explain each attribute type, this topic uses the **Example - Application** panel. However, all the UI definition guidelines apply to the "account" and the "application" sections of the file.

On the Application tab, there is an **Application Type** field. When you select the Example Target Connector for the application type, the **Example - Application** tab becomes available.

The following screen image shows the **Example - Application** tab:

## Update exampleapp

Application	Example - Application
Connect Timeout:	<input type="text" value="60000"/>
Read Timeout:	<input type="text" value="5000"/>
SSH Port:	<input type="text" value="22"/>
Connector Protocol:	<input type="radio"/> SSL <input type="radio"/> TLS 1.0 <input checked="" type="radio"/> TLS 2.0
Additional Encryption:	<input type="text" value="AES"/>
Use Certificate:	<input type="checkbox"/>
Certificate:	<input type="text"/>

How to define the tabs and fields is described in these topics:

- [Define Required uiDefinition and Tabs Sections](#)
- [Define Custom Connector Tabs](#)
- [Create a Number Field](#)
- [Create a Text, Text Area, and Password Attributes](#)
- [Display a Field with Radio Buttons](#)
- [Use a Checkbox to Select an Option](#)
- [Create a Field with a Drop-down List of Values](#)
- [Define the Locale for Field Labels](#)
- [Create a Target Account Selection Field](#)

### **Define Required uiDefinition and Tabs Attributes**

Each application and accounts section requires a "uiDefinitions" attribute followed by a single "tabs" attribute. These attributes designate the following information:

- **uiDefinition** - For each application and account section, this attribute is the parent for the "tabs" definition.
- **tabs** - This section lists an array of tab objects that contain the tab identifier, label, and corresponding "fields" displayed on each tab. This attribute lets you define high-level tabs to group related fields.

The following code example shows these two sections:

```
"application": {
  "uiDefinition": {
    "tabs": [{
      "id": "ExampleAppDetail",
```

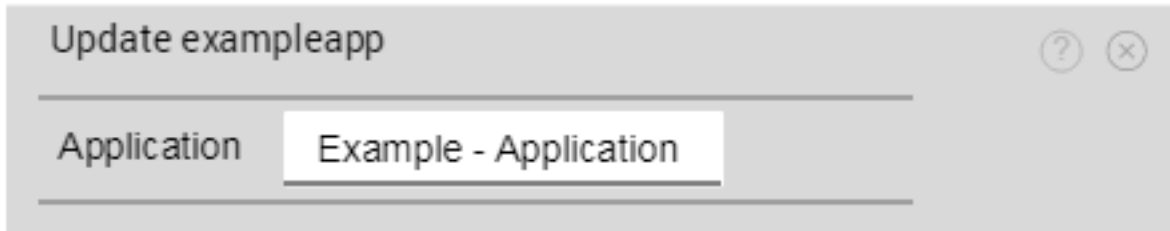
```
"label": "Example - Application",

"fields": [{...}]
```

### Define Custom Connector Tabs

A tab contains all the target application or target account attributes for your target connector. To group related attributes, create one or more tabs as needed.

The following graphic shows the Example - Application tab.



Each tab must have the following attributes:

Attribute	Description
id	Unique identifier for the tab. This identifier must be unique on the UI panel where the tab is rendered. Every identifier must begin with a letter or underscore, followed by one or more letters, underscores or digits. You can follow an initial underscore with another underscore. Valid identifiers are case-sensitive. Tab identifiers cannot contain embedded spaces.
label	The text on the tab itself, such as Example - Application, which is shown in the previous graphic. If the value of the label is an identifier from the "locale" section of the file, the language-specific string is used. If a locale identifier is not specified, the literal string value is used. For more details, see <a href="#">Define the Locale for UI Field Labels</a> later in this topic.
fields	Specifies an array of field objects to display on the tab panel.

To add a target application tab that is labeled Example - Application, use the following JSON syntax:

```
"application": {
  "uiDefinition": {
    "tabs": [{
      "id": "ExampleAppDetail",
      "label": "Example - Application",

      "fields": [{...}]
```

To add the two tabs, **Example - Application** and **User Information**, use the following JSON syntax:

```
"application": {  
  "uiDefinition": {  
  
    "tabs": [{  
  
      "id": "ExampleAppDetail",  
  
      "label": "Example - Application",  
  
      "fields": [{  
  
        "type": "NUMBER",  
  
        "field": "connectTimeout",  
  
        "label": "Connect Timeout",  
  
        "required": false,  
  
        "minValue": 1,  
  
        "value": 60000  
  
      }]  
  
    }, {  
  
      "id": "ExampleAppUserInfo",  
  
      "label": "User Information",  
  
      "fields": [{  
  
        "type": "TEXT",  
  
        "field": "firstName",  
  
        "label": "First Name",  
  
        "required": true  
  
      }], {  
  
        "type": "TEXT",
```

```

        "field": "lastName",

        "label": "Last Name",

        "required": true

    }, {

        "type": "NUMBER",

        "field": "age",

        "label": "Age",

        "required": false,

        "minValue": 1,

        "value": 1

    }]

}

}

```

### Create a Number Field

To display fields that require numerical entries, such as ports, timeouts, add a `NUMBER` field type. You can restrict `NUMBER` fields by specifying a minimum (`minValue`) or maximum (`maxValue`) constraint.

The following JSON syntax creates the Connect Timeout, Read Timeout, and SSH Port fields in the Example - Application panel. Based on the JSON, this panel includes initial default values for each field. The example shows how to provide minimum and maximum restrictions on the specified values. Also, the example has the `required` attribute set to `true`, which indicates that you must specify a value. You cannot leave the attribute blank.

```

"fields": [{
    "type": "NUMBER",
    "field": "connectTimeout",
    "label": "Connect Timeout",
    "required": true,
    "minValue": 1,
    "value": 60000
}, {
    "type": "NUMBER",
    "field": "readTimeout",
    "label": "Read Timeout",
    "required": true,

```



```

        "minValue": 1,
        "value": 5000
    }, {
        "type": "NUMBER",
        "field": "sshPort",
        "label": "SSH Port",
        "required": true,
        "minValue": 0,
        "maxValue": 65535,
        "value": 22
    }
]

```

### Create a Text, Text Area, and Password Attributes

The following excerpt shows the definition for the following field types:

- TEXT: A field that requires text.
- TEXTAREA: A field that can accommodate a large amount of text.
- PASSWORD: A field for a user password.

The TEXT type use pattern constraints. The TEXT type sets the **required** attribute to true, indicating that the field cannot be left blank. The TEXTAREA does not have any pattern constraints.

```

{

    "type": "TEXT",

    "field": "userName",

    "label": "User Name",

    "required": true,

    "minLength": 1,

    "maxLength": 200

}, {

    "type": "TEXT",
    "field": "admin",
    "label": "Administrator",
    "required": true,
    "maxLength": 16,
    "patternConstraint": "^[A-Za-z0-9]+$",
    "patternConstraintMessage": "Administrator name consists of letters and numbers
only",

```

```

    "value": "admin"

  }, {

    "type": "TEXTAREA",

    "field": "certificate",

    "label": "Certificate"

  }, {

    "type": "TEXT",

    "field": "occurance",

    "label": "Activity from",

    "patternConstraint": "^(today|tomorrow|yesterday)$",

    "patternConstraintMessage": "Enter today, tomorrow or yesterday"

  }, {

    "type": "PASSWORD",

    "field": "user_password",

    "label": "User Password"

  }

```

### ***Display a Field with Radio Buttons***

The **RADIO** attribute type displays a control for selecting only one option from a set of a predefined and mutually exclusive option. The **RADIO** type is recommended for a configuration setting with only a few options. The **RADIO** type requires a "values" attribute followed by two or more unique "label" and "value" options for the control.

The following JSON syntax creates the Connector Protocol setting with three options: TLS 1.0, 1.2. and 1.3. When you create a Target Application or Account, the TLS 1.2 option is set by default. If no initial value is specified, the first option, in this example TLS 1.0, is selected by default.

```

{
  "type": "RADIO",
  "field": "connector_protocol",
  "label": "Connector Protocol",
  "value": "TLS_1.2",

```

```

    "values": [{
      "label": "TLS 1.0",
      "value": "TLS_1"
    }, {
      "label": "TLS 1.2",
      "value": "TLS_1.2"
    }, {
      "label": "TLS 1.3",
      "value": "TLS_1.3"
    }
  ]
}

```

### ***Use a Checkbox to Select an Option***

To display a field with a checkbox for a true or false choice, use the CHECKBOX parameter type.

The following JSON syntax creates the Use Certificate field in the Example - Application panel. By default, this panel has the option set to true (selected) by default. If no initial value is provided, the control is false (not selected).

```

{
  "type": "CHECKBOX",
  "field": "certificate",
  "label": "Use Certificate",
  "value": true
}

```

### ***Create a Field with a Drop-down List of Values***

To display a field with values selectable from a drop-down list, add a COMBOBOX parameter type.

The following JSON syntax creates the Additional Encryption field in the Example - Application panel. When creating a target application or account, this example shows AES set as the default value. If no initial value is specified, the first item, in this example Triple DES, is selected by default.

```

{
  "type": "COMBOBOX",
  "field": "additionalEncryption",
  "label": "Additional Encryption",
  "value": "AES",
  "values": [{
    "label": "Triple DES",

```

```

        "value": "TRIPLEDES"
    }, {
        "label": "RSA",
        "value": "RSA"
    }, {
        "label": "Blowfish",
        "value": "BLOWFISH"
    }, {
        "label": "Twofish",
        "value": "TWOFISH"
    }, {
        "label": "AES",
        "value": "AES"
    }
  ]
}

```

### Create a Target Account Selection Field

To create a field where a user can select a target account, use the TARGETACCOUNT field type. This field displays a field with a drop-down list from which to select an account. The field also lets a user search and select a target account. In the following example, on the Example - Account panel, there are two fields, one labeled Description and the other field labeled Master Account.

```

"fields": [{
    "type": "TEXT",
    "field": "description",
    "label": "Description",
    "maxLength": 60
  }, {
    "type": "TARGETACCOUNT",
    "field": "anotherAccount",
    "label": "Master Account"
  }
]

```

### Define the Locale for UI Field Labels

To localize how field labels display in a web browser, add a **locale** section to the uiDefinitions.json file. The locale attribute interacts only with the browser locale. The only supported locale values are **en** (English) and **ja** (Japanese).

Guidelines for the locale section:

- There can be only one locale section in the file
- Under the locale section you can have multiple subsections, one for each language. For example, under locale you can list an "en" subsection and a "ja" subsection.
- For each field label that you want in a specific language, add a corresponding string in the relevant language subsection.
- If you have a label that you cannot localize, such as a proper name, do not include a string in the locale section.

The following table explains how the browser locale and the locale section work together to render UI pages:

Browser Locale	Specified Locale Section in the uiDefinitions.json File	Language Displayed in the PAM UI
English	en	English. All other locale sections in the file are ignored. If the <code>label</code> for a field does not have a corresponding string in the <code>en</code> section, the UI uses the literal value of the label. This value can be any language.
Japanese	ja	Japanese. All other locale sections in the file are ignored. If the <code>label</code> for a field does not have a corresponding string in the <code>ja</code> section, the UI uses the literal value of the <code>label</code> . This value can be any language.
<b>Note:</b> If there is no locale section, the UI displays the literal value of the <code>label</code> for a control. For example, if a label is in Japanese, the field name displays in Japanese even if the browser is set to English.		

You can enter strings in the locale section in two formats. You can mix both formats in the same locale section. The format options are:

- Regular string values. **JSON example:** "AccountTabLabel" : "Account Tab"
- Unicode hexadecimal character. This format begins with a backslash and the letter u (\u), followed by a four-value hexadecimal constant. This format is required for multi-byte languages, such as Japanese.

**JSON Example:** "AccountTabLabel" : "\u30a8\u30b3\u30fc\u30a2\u30ab\u30a6\u30f3\u30c8"

The browser locale determines whether "Account Tab" is rendered in English or rendered in Kanji characters.

The following example is an abbreviated sample JSON file with a locale attribute. The example shows a section for English and Japanese and the regular string and Unicode hexadecimal formats that you can use. The locale section renders four UI panels—an Account Tab in English and Japanese and an Application Tab in English and Japanese. For illustration purposes, the two Account Tab panels are shown.

```

{
  "account": {
    "uiDefinition": {
      "tabs": [{
        "id": "AccountTab",
        "label": "AccountTabLabel",
        "fields": [{
          "type": "TEXT",
          "field": "AccountNameField",
          "label": "AccountNameFieldLabel"
        }]
      }]
    },
  },
  "application": {
    "uiDefinition": {
      "tabs": [{
        "id": "ApplicationTab",
        "label": "ApplicationTabLabel",
        "fields": [{
          "type": "TEXT",
          "field": "ApplicationNameField",
          "label": "ApplicationNameFieldLabel"
        }]
      }]
    },
  },
  "locale" : {
    "en" : {
      "AccountTabLabel" : "Account Tab",
      "AccountNameFieldLabel" : "Account Name",

      "ApplicationTabLabel" : "Application Tab",
      "ApplicationNameFieldLabel" : "Application Name"
    },
    "ja" : {
      "AccountTabLabel" : "\u30a8\u30b3\u30fc\u30a2\u30ab\u30a6\u30f3\u30c8",
      "AccountNameFieldLabel" : "\u30c6\u30ad\u30b9\u30c8\u30d5\u30a3\u30fc",

      "ApplicationTabLabel" : "\u30a8\u30b3\u30fc\u0020\u002d\u0020\u30a2\u30d5\u30c8",
      "ApplicationNameFieldLabel" : "\u756a\u53f7\u30d5\u30a3\u30fc\u30ab\u30c8\u30c9"
    }
  }
}

```

The following screens show the Account Tab in English and Japanese:

Validate TCF Definition

TCF Definition JSON Account Tab

Account Name:

CLOSE

除済みサー

ワードを エコーアカウント

テキストフィールド:

閉じる

### Localization for the Server

The language for request and error messages from PAM and the Custom Connector server is determined by the PAM server. Messages include log and error messages about the TCF and the custom connector, and UI validation errors. If the appliance locale is English, then all error messages that the TCF returns to PAM are in English. If the appliance locale is Japanese, then all the error messages that the TCF returns are in Japanese.

When you update a target connector configuration, the validation request goes to the TCF server. If there are errors, the language that the error messages are displayed is based on the locale of the PAM server.

#### NOTE

Continue by reading about the required [web services endpoints](#).

### Web Service Endpoints for the Custom Connector

Each target connector must support three web service classes:

The Custom Connector software comes with a project named `customConnectorTemplate`. This project includes all three services, which are defined in `com/ca/pam/customConnectorTemplate/api`. Before you develop your own target connector, read about each service class in detail. Then use the `customConnectorTemplate` as a basis to write your own Java code.

### **Credentials Service**

The Credentials service verifies and updates the credentials for an account at the remote target device.

#### **URLs for the Credentials service:**

- `http://tomcat_host:port/capamef/targetConnectors/target_connector_name/credentials/validate`
- `http://tomcat_host:port/capamef/targetConnectors/target_connector_name/credentials/update`

**Method supported:** POST

**Sample REST call:** HTTP POST `http://112.22.30.111:8443/capamef/targetConnectors/exampleTargetConnector/credentials/validate`

The following sample code includes requests to update and verify credentials. The extended attribute sections are based on the account and application attributes defined in `uiDefinitions.json` file.



Figure 32: sample credentials.java

**Update credential**

```

{
  "oldPassword": "xxxxxxxxxxxxx",
  "account":
  {
    "accessType": null,
    "privileged": true,
    "password": "xxxxxxxxxxxxx",
    "application":
    {
      "targetServer":
      {
        "hostName": "1.1.1.1",
        "ipaddress": "1.1.1.1",
        "deviceName": "exampleDevice"
      },
      "name": "ExampleApplication",
      "type": "exampleTargetConnector",
      "extendedAttributes":
      {
        "sshPort": "22",
        "additionalEncryption": "AES",
        "connector_protocol": "TLS_2",
        "readTimeout": "5000",
        "useCertificate": "false",
        "connectTimeout": "60000",
        "certificate": ""
      }
    },
    "cacheAllow": true,
    "cacheDuration": 30,
    "userName": "test",
    "extendedAttributes":
    {
      "description": "Example description",
      "admin": "admin",
      "adminPassword": "xyyyzzaa!!"
    },
    "cacheBehavior": "useCacheFirst",
    "synchronize": true
  }
}

```

**account attribute** (points to the "account" field)

**application attribute** (points to the "application" field)

**Verify credential** }

```

{
  "account":
  {
    "accessType": null,
    "privileged": true,
    "password": "xxxxxxx",

```

## UIDefinitions Service

The UIDefinitions service returns UI definitions in JSON format for a specified field type. This service determines how the Java code and the JSON file work together.

**URL for the uiDefinitions service:** `http://tomcat_host:port/capamef/targetConnectors/target_connector_name/uiDefinitions/{uiDefinitionType}`

In the uiDefinitions service URL:

- `tomcat_host:port` values are not case-sensitive.
- `target_connector_name` must be in lower camel case. For example, `customTargetConnector`.
- `uiDefinitionType` must be **account** or **application**

**Method supported:** GET

**Sample REST call:** HTTP GET `http://112.22.30.111:8443/capamef/targetConnectors/exampleTargetConnector/uiDefinitions/application`

**Sample Response from the TCF:**

```
{ "_data": { "application": { "uiDefinition": { "tabs": [ { "label": "Example -
Application", "id": "ExampleAppDetail",

"fields": [ { "type": "NUMBER", "field": "connectTimeout", "minValue": "1", "label": "Connect
Timeout", "required": false, "value": "60000" },

{ "type": "NUMBER", "field": "readTimeout", "minValue": "1", "label": "Read
Timeout", "required": false, "value": "5000" },

{ "type": "NUMBER", "field": "sshPort", "minValue": "0", "label": "SSH
Port", "required": false, "value": "22", "maxValue": "65535" },

{ "type": "RADIO", "field": "connectorProtocol", "label": "Connector
Protocol", "required": false, "value": "TLS_1.2",

"values": [ { "label": "TLS 1.0", "value": "TLS_1" }, { "label": "TLS 1.2", "value": "TLS_1.2" },
{ "label": "TLS 1.3", "value": "TLS_1.3" } ] },

{ "type": "COMBOBOX", "field": "additionalEncryption", "label": "Additional
Encryption", "required": false, "value": "AES",

"values": [ { "label": "Triple DES", "value": "TRIPLEDES" }, { "label": "RSA", "value": "RSA" },
{ "label": "Blowfish", "value": "BLOWFISH" },

{ "label": "Twofish", "value": "TWOFISH" }, { "label": "AES", "value": "AES" } ] },

{ "type": "CHECKBOX", "field": "useCertificate", "label": "Use
Certificate", "required": false, "value": "false" },

{ "type": "TEXTAREA", "field": "certificate", "label": "Certificate", "required": false } ] ] ] ] } }, "_meta": {
"_success": "true" } }
```

## Validations Service

The Validations service verifies account and application data before saving it into the Privileged Access Manager database.

**URL for the Validations service:** `http://tomcat_host:port/capamef/targetConnectors/target_connector_name/validations/{validationType}`.

- If the *validationType* is **account**, this service validates data for target account creation and update.
- If the *validationType* is **application**, this service validates data target application creation and update.

**Methods supported:** POST, PUT

**Sample REST call:** HTTP POST `http://112.22.30.111:8443/capamef/targetConnectors/exampleTargetConnector/validations/application`

The following sample request payload includes requests to the Validations service. The extended attributes in the payload are defined in the previous sample response for the uiDefinitions service.

### Sample Request Payload:

```
"application": {
  "targetServer": {
    "hostName": "114.20.50.111",
    "ipaddress": "114.20.50.111",
    "deviceName": "UnixDevice"
  },
  "name": "UnixApp",
  "type": "exampleTargetConnector",
  "extendedAttributes": {
    "sshPort": "22",
    "additionalEncryption": "AES",
    "connectorProtocol": "TLS_1.2",
    "readTimeout": "5000",
    "useCertificate": "false",
    "connectTimeout": "60000",
    "certificate": ""
  }
}
```

A `ValidationManager` class is distributed in the core library. This class validates data based on the constraints in the `uiDefinitions` JSON file. In additions to these standard validations, you can add custom validations to this class. If a validation fails, the `ValidationManager` class throws an `ExtensionException` with a list of messages.

To see sample code, look at the `Validations.java` class in the `customConnectorTemplate` project.

### NOTE

Now that you are familiar with the components for creating a custom target connector, [Build Your Custom Connector](#).

## Build Your Custom Connector

Now that you are familiar with the UI definitions and the web service endpoints, you can build your own connector.

Follow these steps in order:

### NOTE

All custom target connectors must be installed on every instance of the Custom Connector server. You can install the Custom Connector server on a Windows or Linux system as long as the Tomcat server is installed on that system. If your custom target connector code is using native operating system calls, then all target connectors must make calls to that same operating system. Do not write one target connector that makes native Windows calls and another target connector that makes native Linux calls. One of the connectors fails because they are operating on one server

### Deploy the Custom Connector Software

Before you build a custom connector, complete the steps in [Deploy the Custom Connector Software](#). Ensure that you configured the settings on the Custom Connector page (**Configuration, Custom Connectors**).

### Obtain the Required Software

- JDK 8 Update 201 (minimum version) or JDK 11
  - Java build tool: Apache Maven or Gradle
  - Core library `com.ca.pam:capamexternsionscore:4.16.0`, included with the SDK, in the directory `sdk/lib`.
  - Repository for Maven or Gradle
- Maven and Gradle rely on a repository to manage library dependencies. To create a connector project, first set up a repository with the following dependencies:

JDK 8	JDK 11
<ul style="list-style-type: none"> <li>• <code>javax.ws.rs:javax.ws.rs-api:2.0.1</code></li> <li>• <code>org.glassfish.jersey.containers:jersey-container-servlet:2.25.1</code></li> <li>• <code>org.glassfish.jersey.media:jersey-media-json-jackson:2.25.1</code></li> <li>• <code>org.codehaus.jettison:jettison:1.3.8</code></li> <li>• <code>io.swagger:swagger-jersey2-jaxrs:1.5.19</code></li> <li>• <code>org.slf4j:slf4j-api:1.8.0-beta2</code></li> <li>• <code>org.apache.logging.log4j:log4j-api:2.11.0</code></li> <li>• <code>org.apache.logging.log4j:log4j-core:2.11.0</code></li> <li>• <code>org.apache.logging.log4j:log4j-slf4j-impl:2.11.0</code></li> </ul>	<ul style="list-style-type: none"> <li>• <code>org.glassfish.jersey.containers:jersey-container-servlet:2.27</code></li> <li>• <code>org.glassfish.jersey.core:jersey-common:2.27</code></li> <li>• <code>org.glassfish.jersey.inject:jersey-hk2:2.27</code></li> <li>• <code>org.glassfish.jersey.media:jersey-media-multipart:2.27</code></li> <li>• <code>javax.xml.bind:jaxb-api:2.3.1</code></li> <li>• <code>javax.activation:activation:1.1.1</code></li> <li>• <code>org.glassfish.jersey.media:jersey-media-json-jackson:2.27</code></li> <li>• <code>org.codehaus.jettison:jettison:1.4.0</code></li> <li>• <code>io.swagger:swagger-jersey2-jaxrs:1.5.21</code></li> <li>• <code>javax.servlet:javax.servlet-api:4.0.1</code></li> </ul>

### Create a Project for the Custom Connector

The first step before building the custom target connector is to create a project for the connector. The Custom Connector zip includes a command-line script to create a project for your custom connector:

**Windows:** `createTCProject.cmd`

**UNIX:** `createTCProject`

When you run the `createTCProject` script, it uses the `custom ConnectorTemplate` to build the project. The `customConnectorTemplate` contains metadata files for the Maven and Gradle source code. The template also contains example source code for creating the input validation service and the credentials verification and update services.

**NOTE**

If you set the JAVA\_HOME environment variable on the system where you run the createTCProject script, the script reads the JDK path from this variable. Ensure that the script is pointing to the correct JDK version and update.

**To create a project:**

Go to the directory that contains the script, then execute the following command:

```
createTCProject -Dworkspace=workspace_location -DgroupId=group_id -
DartifactId=project_id -Dversion=version -DbuildTool=build_tool
```

The command example is for UNIX platforms. For Windows systems, other than the command extension, the command is the same.

Alternatively, specify an absolute or relative path to the script. For example, if you are at the directory C:\CAPAM\customconnectors and the file is in \CAPAM\sdk, the command using the absolute path is:

```
C:\CAPAM\sdk\createTCProject -Dworkspace=workspace_location -DgroupId=group_id -
DartifactId=project_id -Dversion=version -DbuildTool=build_tool
```

The command using the relative path is:

```
..\sdk\createTCProject -Dworkspace=workspace_location -DgroupId=group_id -
DartifactId=project_id -Dversion=version -DbuildTool=build_tool
```

The place holders in italicized text get replaced with the following information:

- *workspace\_location*: The location where the target connector project is generated. This path can be a relative or absolute path. If this folder does not exist, the tool creates it.
- *group\_id*: The group Identifier for the target connector project, like the Maven or Gradle group identifier. This ID is also used as the package prefix for the project Java source files.
- *artifact\_id*: The name of the target connector project. A folder with this name is created in the workspace. All the source files and project files for target connector are generated in this folder. This ID is also used in the generated package name.
- *version*: The version of the target connector project.
- *build\_tool*: Indicates which build tool (Maven or Gradle) to use for the target connector project.

**Create a project – Gradle Example:**

```
createTCProject -Dworkspace=tcworkspace -DgroupId=com.company.tc -
DartifactId=myconnector -Dversion=1.0 -DbuildTool=gradle
```

**Create a project – Maven Example:**

```
createTCProject -Dworkspace=tcworkspace -DgroupId=com.company.tc -
DartifactId=myconnector -Dversion=1.0 -DbuildTool=maven
```

After you create a project, the following directory structure is created from where you ran the command:

**Figure 33: custom connector gradle project structure****tcworkspace**

```

| ..... application
|   | ..... gradle
| ..... src
|   | ..... main
|       | ..... java
|           | ..... com/company/tc/myconnector/api
|               | ..... credentials.java
|               | ..... UIDefinitions.java
|               | ..... Validations.java
|           | ..... resources
|               | ..... extension_messages.properties
|               | ..... extensions.properties
|               | ..... TargetConnectorMessages_en_US.properties
|               | ..... TargetConnectorMessages_ja.properties
|               | ..... uiDefinitions.json
|           | ..... webapp
|               | ..... WEB-INF
|                   | ..... web.xml
|               | ..... META-INF
|               | ..... index.html
| ..... build.gradle
| ..... gradlew.bat
| ..... gradlew

```

After you create a project, build a custom target connector.

## **Build the Custom Connector using a Build Script**

The Custom Connector zip includes scripts for building a custom connector.

Build the connector, following the instructions for one of the following build scripts:

- [Run the Gradle Build Script](#)
- [Run the Maven Build Script](#)

### **Run the Gradle Build Script**

The template includes a **build.gradle** build script. This file includes repositories, dependencies, and plug-in configurations. A sample of the build.gradle script is shown after the procedure.

Modify the script as instructed:

1. Modify the `repositories` section and include your repository.  
The `repositories` section includes the Maven central repository. The `mavenCentral` repository can remain in the script or you can remove it.
2. List dependencies in the `dependencies` section. The list must include dependencies on the target connector core library and on any other third-party libraries that the core library requires. All the dependencies that you add in this section must be installed in your repository so that the libraries are available to Gradle build script.

The default build.gradle script is shown in the following graphic:

```
buildscript {
    repositories {
        mavenCentral()
    }
}

apply plugin: 'war'
apply plugin: 'eclipse-wtp'
apply plugin: 'idea'
sourceCompatibility = 1.8
targetCompatibility = 1.8

repositories {
    mavenCentral()
}

dependencies {
    compile ('javax.ws.rs:javax.ws.rs-api:2.0.1')
    compile ('org.glassfish.jersey.containers:jersey-container-servlet:2.25.1')
    compile ('org.glassfish.jersey.media:jersey-media-json-jackson:2.25.1')
    compile ('org.codehaus.jettison:jettison:1.3.8')
    compile ('io.swagger:swagger-jersey2-jaxrs:1.5.19')
    compile ('org.slf4j:slf4j-api:1.8.0-beta2')
    compile ('org.apache.logging.log4j:log4j-api:2.11.0')
    compile ('org.apache.logging.log4j:log4j-core:2.11.0')
    compile ('org.apache.logging.log4j:log4j-slf4j-impl:2.11.0')
    compile ('com.ca.pam:capamextensionscore:4.16.0')
}

file('build').mkdirs()

war {
    archiveName 'projectTemplate.war'
}
```

3. After you finish modifying the Gradle build script, run the script using the following command:

```
gradlew.bat build
```

If the build is successful, a **.war** file is created in the build directory. If there is a problem with the build, error messages display in the console. Make the necessary corrections and rerun the script.

4. Import the Gradle project into your integrated development environment (IDE), such as Eclipse or IntelliJ.
5. Go to the next task, [Modify the uiDefinitions.json File](#).

### **Run the Maven Build Script**

The template includes a **pom.xml** file. This file includes repositories, dependencies, and plug-in configurations.

Modify the script as instructed:

1. Modify the `repositories` section and include your repository.  
The `repositories` section includes the Maven central repository. The `mavenCentral` repository can remain in the script or you can remove it.
2. List dependencies in the `dependencies` section. The list must include dependencies on the target connector core library and on any other third-party libraries that the core library requires. All the dependencies that you add in this section must be installed in your repository so that the libraries are available to maven build script.

The default Maven `pom.xml` file is shown in the following graphic:

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>com.ca.pam</groupId>
  <artifactId>customConnectorTemplate</artifactId>
  <version>1.0</version>
  <repositories>
    <!-- Define corporate repository here.-->
  </repositories>
  <dependencies>
    <dependency><groupId>javax.ws.rs</groupId><artifactId>javax.ws.rs-api</
artifactId><version>2.0.1</version></dependency>
    <dependency><groupId>org.glassfish.jersey.containers</groupId><artifactId>jersey-
container-servlet</artifactId><version>2.25.1</version></dependency>
    <dependency><groupId>org.glassfish.jersey.media</groupId><artifactId>jersey-media-
json-jackson</artifactId><version>2.25.1</version></dependency>
    <dependency><groupId>org.codehaus.jettison</groupId><artifactId>jettison</
artifactId><version>1.3.8</version></dependency>
    <dependency><groupId>io.swagger</groupId><artifactId>swagger-jersey2-jaxrs</
artifactId><version>1.5.19</version></dependency>
    <dependency><groupId>org.slf4j</groupId><artifactId>slf4j-api</
artifactId><version>1.8.0-beta2</version></dependency>
    <dependency><groupId>org.apache.logging.log4j</groupId><artifactId>log4j-api</
artifactId><version>2.11.0</version></dependency>
    <dependency><groupId>org.apache.logging.log4j</groupId><artifactId>log4j-core</
artifactId><version>2.11.0</version></dependency>
```



```

    <dependency><groupId>org.apache.logging.log4j</groupId><artifactId>log4j-slf4j-impl</artifactId><version>2.11.0</version></dependency>
    <dependency><groupId>com.ca.pam</groupId><artifactId>capamextensionscore</artifactId><version>4.16.0</version></dependency>
    <!-- Add additional dependencies -->
</dependencies>
<plugins>
    <plugin>
        <artifactId>maven-war-plugin</artifactId>
        <version>2.3</version>
    </plugin>
</plugins>
</project>

```

3. After you finish modifying the Gradle build script, run the script using the following command:

```
mvmw.cmd package
```

If the build is successful, a **.war** file is created in the target directory. If there is a problem with the build, error messages display in the console. Make the necessary corrections then rerun the script.

4. Import the Maven project into your integrated development environment (IDE), such as Eclipse or IntelliJ.
5. Go to the next task, [Modify the uiDefinitions.json File](#)

### **Modify the uiDefinitions.json File**

In the project you created, add, or modify the tab and field attributes to render all the necessary UI elements for your custom target connector.

#### **Follow these steps:**

1. In your project, navigate to the directory **/src/main/resources/** and locate the uiDefinitions.json file.
2. Open the file in a JSON editor and modify the entries for your custom connector.
3. Define an "application" section and "account" section. The application extended attributes enable communication to the target device. The account section extended attributes verify or update account credentials at the target device.

For detailed information about valid UI attributes, see [UI Fields and Controls for Configuring Connectors](#).

### **Test and Validate the UI Definitions**

The UI provides a mechanism for testing and validating the attributes in the uiDefinitions.json file. The validation mechanism can also test the creation and modification of the target application and account user interface controls. The facility verifies whether the syntax and structure of the JSON entries are correct. If there are any errors with a definition, error messages are displayed from the UI. These messages can indicate problems with syntax or other issues in the uiDefinitions.json file. You can also define custom validation rules. Custom validation can contain field validation criteria, which verifies UI data when users update or can save the target application or account.

The facility also has a preview option. After you modify the uiDefinitions.json file, you can see the resulting UI panels and controls for the target application and account.

#### **NOTE**

Only administrators with the Target Connector Validator role can use the validation facility. The Target Connector Validator role is assigned the Validate Target Connector UI privilege.

#### **To validate the UI definitions, follow these steps:**

1. Log in to the UI as an Administrator with the **Target Connector Validator** role, such as an Operational Administrator.

You must be assigned a role with the Validate Target Connector UI privilege to see the Validate TCF Definition option under the **Settings** menu.

2. Select **Settings, Validate TCF Definition**.

The Validate UI Definition page displays with a **TCF Definition JSON** page.

3. Copy and paste the content from a uiDefinitions.json file to the page.

Alternatively, you can manually enter the JSON for the application and account tabs and other UI elements. Follow the JSON syntax and expected field attributes, as described earlier in this topic.

4. After you put content on the page, select **Validate**.

The syntax of the definitions is examined. If the JSON has any errors, the facility reports these errors to the user.

### NOTE

Correct any errors that are detected. If any UI definition errors exist, the preview does not display.

5. Preview the application and account panels:

- a. To display the target application panel, select **Show TCF Application**. The panel displays next to the TCF Definition JSON page. The controls reflect what you defined in the application section of the JSON file.
- b. To display the target account panel, select **Show TCF Account**. The panel displays next to the TCF Definition JSON page. The controls reflect what you defined in the account section of the JSON file.

6. To view and update the JSON entries, edit them in the TCF Definition JSON page.

7. After the JSON is complete, copy the text and paste into the **uiDefinitions.json** file.

## Edit the Web Service Endpoints

In the project you created, modify the web service classes that define the endpoints for a custom target connector.

### Follow these steps:

1. In your project, navigate to the directory **/src/main/java/com/company/tc/project\_name/api**. This folder contains three web service classes. Modify only the following two classes:
  - **Credentials.java** - this code provides the business logic that the TCF uses to verify and change passwords at remote endpoints.
  - **Validations.java** - this code validates any field types against the application and account constraints in the uiDefinitions.json file.

Do not modify the UDefinitions.java web service.

2. Edit the **Credentials.java** file. This class provides two stub methods for adding credential verification and update logic for a target connector.

Add your credential verification logic to this stub method:

```
private void processCredentialVerify () throws ExtensionException {
    add credential verification logic here
}
```

Add your credential update logic to this stub method:

```
private void processCredentialUpdate () throws ExtensionException {
    add credential update logic here
}
```

If any of the verifications or updates fail, these methods must throw an ExtensionException.

### NOTE

The data that is required to perform verifications and updates is available as instance variables. These variables are listed in the Credentials.java class.

3. Optionally, modify the **Validations.java** file. This service class validates target application and account data based on the constraints in the uiDefinitions.json file. This class provides the following stub method for adding custom validations.

If you want to add more validations, add your validation logic to this stub method:

```
private void performCustomValidation(Map<String,String> extendedAttributes, String
    validationType) throws ExtensionException {
    add custom validation logic here
}
```

This method takes two arguments:

- **extendedAttributes**: Represents the "field" attribute and its value in the uiDefinitions.json file. The values are the inputs that the user provides in the PAM UI.
- **validationType**: Indicates whether the data is for a target application or a target account. The value can be "account" or "application." The value for the validationType comes from the request URL that is sent by the appliance to the TCF.

If any of the validations fail, this method must throw an ExtensionException.

Here is an example of server-side validation. The following code adds custom validation for a Checkbox control on the Echo - Application panel.

```
private void customValidation(String json, String validationType)
    throws ExtensionException {
    if (validationType.equals("application")) {
        try {
            JSONObject jsonObj = new JSONObject(json);
            JSONObject jobject = jsonObj.getJSONObject(validationType);
            JSONObject jsonObject = jobject.getJSONObject("extendedAttributes");

            if(jsonObject.get("checkboxControl").equals("true")) {
                String str = jsonObject.get("textareaControl").toString();
                if(str.isEmpty() || str.equals("")) {
                    buildException(EchoMessageConstants.TEXTAREA_CONTROL_MISSING, false,
                        "textareaControl");
                }
            }
        } catch (JSONException e) {
            LOGGER.log(Level.SEVERE, "Custom validation failed " + e.toString());
            buildException(MessageConstants.INVALID_JSON, false);
        }

        if(exception != null) {
            throw exception;
        }
    }
}
```

If the validation fails, the following message displays:



For detailed information about the web service endpoints, see [Web Service Endpoints for the Custom Connector](#).

### **Establish Logging for the Custom Connector**

To monitor activity and troubleshoot problems between the appliance and the Custom Connector server, set up logging. The TCF and the example target connectors use the standard

```
java.util.logging
```

package and write messages to the catalina.out file.

When you write log statements, add the following two TCF-specific attributes to the standard log message format. Include these two attributes in all the log statements from the Custom Connector server and custom target connectors so you can debug any issues.

- **request ID**—When PAM generates a request to the Custom Connector server, this auto-generated attribute gets added to the header of every REST web service call. The request ID enables you to track the transaction to and from the Custom Connector server, which helps troubleshoot errors.
- **context name**—When the Custom Connector server writes a message to the log file, the context name identifies whether the source of the message is the TCF or the custom target connector. The context name is configurable. To change the name, go to *Tomcat\_home*\src\main\webapp\WEB-INF\ and edit the name in the web.xml file. The context name is only for logs that the Custom Connector server generates, not PAM.

The following graphic shows the format of log statement. The request id and the context name are preceded and followed by the custom strings that you specify:

```
day-month-year time log_level [url_custom_connector_server] tcf_java_class [request_id]
[context_name]
Forward the request to UIDefinitions
```

For example:

```
01-Nov-2018 13:15:20.735 INFO [http-nio-8080-exec-1]
com.ca.pam.extensions.framework.api.TargetConnectors.targetConnectorUIDefinitions
```

```
[7dc53df5-703e-49b3-8670-b1c468f47f1f] [targetconnector] Forward the request to
UIDefinitions
```

### Add Log Statements to Your Java Code

To add log statements for your custom target connectors, call the `java.util.logging` API. Before calling this API, call the `LoggerWrapper` class to add the request ID and context name to the log messages. For example:

```
LOGGER.log(Level.INFO, LoggerWrapper.logMessage("<message>"));
```

In this example, `LOGGER` is an instance of the `java.util.logging.Logger` class.

#### NOTE

No instance of the `LoggerWrapper` class is required because `logMessage` is a static method. The custom message can be passed as a parameter to the `logMessage` method. The method constructs the log statement by adding the request id and the context name.

### Set Log Levels

When log messages are displayed in the `catalina.out` file, the messages are ordered based on the log level hierarchy. You can change log levels for your messages depending on the level of detail you want reflected in each log message. To modify the log levels, go to the Tomcat server directory `/conf/logging.properties`.

If a particular log level is required for only certain classes in the package, then add the package name to the `logging.properties` file.

### Configure Error Handling for a Custom Connector

The Custom Connector SDK includes error messages that are related to TCF operation. If an error occurs, the TCF sends back to PAM. TCF error messages are in the **`extension_messages.properties`** and the **`extension_messages_ja.JP.properties`** files.

#### NOTE

Do not modify the `extension_messages.properties` files.

For your custom target connectors, you can set up custom error handling specifically for target connector operation. If an error occurs, the target connector sends messages to the TCF which forwards them back to PAM.

Custom error handling reads the error messages from one of the following properties files:

- `artifact_ID_messages.properties` file (English messages)
- `artifact_ID_messages_ja_JP.properties` file (Japanese messages)

When you run the command to create a TCF project, the command automatically creates these two custom properties files in the directory `tomcat_home/src/main/resources`. Any custom message that you write must be added to the message properties file.

### How to Add Custom Error Messages

When you add error messages to the properties file, begin each message with a unique numbered identifier, for example PAM-TC-1001. As you add messages, we recommend using the next number in consecutive order.

#### TIP

Use a different numbering scheme from the numbering in the **`extension_messages.properties`** and the **`extension_messages_ja.JP.properties`** files so the identifiers do not override one another. For example, if the numbering in the `extension_message.properties` file begins with PAM-EF-001, use xxx-xx-1001 for your custom properties file.

You might want comment on the numbering scheme in the custom properties file so the pattern is clear to anyone modifying the file. For example:

```
// Resource Bundle for Custom Target Connector Messages
// Please start the message codes at 1001 (i.e. PAM-TC-1001) to avoid message number
// collisions
// Example: PAM-TC-1001=Text area control must not be empty when checkbox is selected.
```

For error messages related to the TCF and the custom target connector, the locale setting of the PAM appliance determines the language. If the appliance locale is English, then all error messages are in English. If the appliance locale is Japanese, then all messages are in Japanese. In general, any data that is stored in the appliance database is impacted by the appliance locale and not the browser.

### **Complete the Build Process**

1. After you complete all the tasks to build the connector, rebuild your project by entering the Gradle or Maven build command:  
 - gradlew.bat build  
 - mvnw.cmd package  
 An updated *project\_name*.war file is generated.
2. Deploy the *project\_name*.war file by copying the file to the directory */tomcat\_home/webapps\_targetconnectors*. The .war file automatically deploys. The Tomcat server does not have to be restarted.
3. To verify a successful deployment, log in to the Tomcat server where the TCF is deployed. Open the **catalina.out** file and look for a message that reads:  
 Registering client of type, targetConnectors, with name: *project\_name*
4. Log in to the PAM UI as a Global Administrator, Configuration Manager.
5. Select **Configuration** on the top menu.
6. Verify that you see the **Custom Connectors** option in the left pane.
7. Select **Credentials, Manage Targets, Application**.
8. Select **Add**.
9. In the **Application Type** field, confirm that the drop-down list includes the project name of your custom connector.
10. Exit from the UI.

### **Configure Remote Targets with Your Custom Connector**

Now that you have built and deployed your own target connector, you can use the connector to manage privileged account credentials. The procedure for configuring target applications and accounts using a custom connector is the same procedure as it is for out-of-the-box connectors. For instructions, see [Protect Privileged Account Credentials](#).

## **Configure Custom Connectors Using the CLI**

Custom target connectors can be configured using any existing CLI commands that are related to target applications and target accounts. For a list of CLI commands, see [Credential Manager CLI Commands](#).

To execute these types of commands using a custom target connector, add the value of the **field** attribute from the uiDefinitions.json file to the command. The field attribute must match the entry in the JSON file. For each attribute you want to specify, add the string **Attribute.field\_string="value"** separated by a space.

### **TIP**

Use the value of the "field" attribute, not the "label" attribute.

For example, if the uiDefinitions.json file has the following entries in the application section, the CLI command must contain the strings `Attribute.connectTimeout="1 Attribute.sshPort="22"`

```

}, {
    "type": "NUMBER",
    "field": "connectTimeout",
    "label": "Connection Timeout",
    "required": true,
    "minValue": 1,
    "value": 60000

}, {
    "type": "NUMBER",
    "field": "sshPort",
    "label": "SSH Port",
    "minValue": 0,
    "maxValue": 65535,
    "value": 22

```

### Follow this process to use the CLI:

1. Complete *all* the tasks for developing a custom connector.

#### NOTE

To use the CLI commands, you must still define the UI elements in the uiDefinitions.json file.

2. Configure your custom target application and account using the relevant CLI command. The following examples show how to use the addTargetApplication and addTargetAccount commands to add the Example Target Connector.

#### Add a target application:

```

capam_command capam=11.323.23.130 adminUserID=admin cmdName=addTargetApplication
    TargetServer.hostName=myhost.mydomain.com

TargetApplication.name=exampleapp TargetApplication.type=exampleTargetApplication
    Attribute.descriptor1="headquarters"

Attribute.descriptor2="lab" Attribute.sshPort="22" Attribute.connectTimeout="1"

```

#### Add a target account:

```

capam_command capam=11.323.23.130 adminUserID=admin cmdName=addTargetAccount
    TargetServer.hostName=myhost.mydomain.com

TargetApplication.name=exampleapp TargetApplication.type=exampleTargetConnector
    TargetAccount.userName=sysop1 TargetAccount.password=sys0p2

```

```
Attribute.descriptor1="headquarters"
Attribute.descriptor2="lab" Attribute.description="customconnector"
Attribute.anotherAccount="1"
```

3. Follow the same pattern for any other target application or account CLI commands.
4. Verify that your changes with the CLI are working:
  - a. Log in the UI.
  - b. Navigate to **Credentials, Manage Targets, Target Applications**. Select the drop-down list in the **Application Type** field and confirm that you can see the new custom target applications and accounts.
  - c. Navigate to **Credentials, Manage Targets, Target Accounts**. Verify that your custom target account is in the accounts list.

## Troubleshoot Custom Connector Issues

The two components that might require troubleshooting are the Custom Connector Server, where the TCF is running, and the PAM appliance. If there are communication problems between these two components, those issues might also require problem solving.

The following topics offer solutions for common Custom Connector Server and TCF problems:

### Custom Connector (Tomcat) Server Startup Issues

The Custom Connector (Tomcat) server might not start up cleanly or fails to start services. To determine the problem, look for errors in the Tomcat catalina.out log.

Potential reasons for a startup issue include:

- [Property source error](#)
- [Connector is not initializing](#)
- [Authentication header cannot be decrypted](#)
- [Network port issues](#)
- [TLS connection issues](#)

#### ***Problem Loading the Property Source***

The TCF uses its own property source to read the encrypted keystore password from the catalina.properties file. The TCF decrypts the password before giving it to the Tomcat server to access the TLS keystore.

**Error:** If you see the following exception:

```
25-Apr-2019 13:37:57.382 SEVERE [main] org.apache.tomcat.util.digester.Digester.<clinit>
Error loading property source [com.ca.pam.extensions.tcfcryptoutil.TCFPropertySource]
java.lang.ClassNotFoundException: com.ca.pam.extensions.tcfcryptoutil.TCFPropertySource
```

**Action:** Verify that you copied the capamextensionstcfCryptoUtil-x.x.x.jar file to \$CATALINA\_HOME/lib.

#### ***Server Cannot Initialize the Connector Component***

**Error:** If you see the following exception:



```
25-Apr-2019 14:46:50.353 SEVERE [main]
org.apache.catalina.util.LifecycleBase.handleSubClassException Failed to initialize
component [Connector[HTTP/1.1-8443]]
org.apache.catalina.LifecycleException: Protocol handler initialization failed
```

**Actions:** Examine the server.xml file. Verify that the file is showing the correct full path to the TLS keystore on the Custom Connector server. Also, ensure that the keystore password correct. The keystore password must be set to the `#{tomcat.keystore.pwd}` property, which is specified the catalina.properties file.

### **Authorization Header Cannot be Decrypted**

**Error:** If you see the following exception:

```
25-Apr-2019 14:52:48.157 SEVERE [https-jsse-nio-8443-exec-6]
com.ca.pam.extensions.framework.util.ExtensionAuthenticationFilter.validateAuthToken
[5435a4b9-9c8c-4e6a-b1d8-eef45857569b] [PAMTargetConnector] Authorization header cannot
be decrypted:
org.jose4j.lang.InvalidKeyException: The key must not be null.
```

### **Actions:**

- Verify that the extension.encryption.pwd is set in the extension\_framework.properties file
- Verify that the extension.keystore.file is set in the extension\_framework.properties. Ensure that the file path is correct.
- Ensure that a keystore exists on the Custom Connector server and ensure that the encryption key is in the keystore.

### **Network Port Issues**

See if the Custom Connector Server is listening on the following network ports:

- Port 8080 for any address
- Port 18080 for loopback address (127.0.0.1:18080)
- If TLS enabled, port 8443 for any address

To determine which processes are bound to the network ports, run the following command for your platform:

**Linux:** `netstat -tulpn`

**Windows:** `netstat -aon`

This Windows command requires administrative privileges.

The ports that are specified in the server.xml file must display in the `netstat` command output. If the ports are not displayed, verify that the Custom Connector Server is running. Also ensure that the services that are associated with the ports have started. If the Tomcat server is using non-default ports, ensure that these non-default ports are listed in the `netstat` output. If the ports are not, ensure that they are defined in the server.xml file.

### **TLS Connection Issues**

If you enabled TLS for the Custom Connector configuration, verify that the catalina.properties file has the correct values for the appropriate properties. The appropriate properties are:

- `org.apache.tomcat.util.digester.PROPERTY_SOURCE`
- `tomcat.keystore.pwd`

If you see the following exception in the PAM Tomcat log `java.net.NoRouteToHostException: No route to host (Host unreachable)`, run the `tracert` command. The `tracert` command determines whether the

appliance has line-of-site to the Custom Connector Server. If the server is reachable, then the TLS properties are the issue. Verify these properties.

### **Custom Connector Server Operational Issues**

All Custom Connector Framework diagnostic information in tomcat log (catalina.out). The level of diagnostic and Java package-specific diagnostics are defined in the logging.properties file. This file is in the directory \$CATALINA\_HOME/conf. The default log level is INFO.

For example: com.ca.pam.extensions.framework.level = INFO

When reviewing the log, knowledge of Tomcat and Java logging is helpful.

### **PAM Appliance Issues**

At PAM, the two main areas to focus on for troubleshooting are the PAM Tomcat server and the UI.

#### ***Review the Tomcat Log***

To review operation at the appliance, look at the PAM Tomcat log, catalina.out. Most of the diagnostic information is in this log. If you suspect communication problems, this log is also where you can look. The appliance initiates all communication, except for A2A transactions.

You can control the **Tomcat Log Level** from the UI. Select to **Configuration, Diagnostics, Diagnostic Logs**. The default level is Warning.

The screenshot shows the 'Log Levels' tab in the PAM UI. A dropdown menu is open for 'Tomcat Log Level', displaying the following options: Warning (highlighted), Severe, Info, Config, Fine, Finer, Finest, and Off. Other log level settings listed on the left include CA PAM as SAML RP Log Level, CA PAM as SAML IdP Log Level, Web Services Log Level, LDAP Sync Log Level, and Applet Log Level.

Most TCF-specific diagnostics are from the classes CustomConnectorUtil and CustomConnectorResult.

### ***UI Issues***

**Issue:** You are seeing JavaScript errors when rendering the UI.

#### **Actions**

- Enable UI Logging. Select **Configuration, Diagnostics, UI Log** and configure the UI Log Settings. To see the log results, select the **UI Log Entries** tab.
- Verify the integrity of the uiDefinitions.json file. Select **Settings, Validate TCF Definition** to use the validator utility. For more instructions, see [Build Your Custom Target Connector](#), and read the section **Test and Validate the UI Definitions**.

**Issue:** Building target applications or target accounts for custom connectors can produce errors. The errors are displayed as popup messages on the target application or target account UI page. Errors can range from the target connector not being registered to a custom error message coded by a connector developer.

**Action:** Look at the popup message for information about the source of the problem. If the popup is from a message from the TCF, the address of the Custom Connector server is included. Look at the logs and the configuration of the Custom Connector server.

**Issue:** Testing the Custom Connector connection fails. You used the **Test** button on the Configuration, Custom Connector page, and the test failed.

**Actions:**

- Verify the configuration settings on the Custom Connector page.
- Examine the PAM Tomcat catalina.log for communication errors, such as timeouts and connection refused
- Look at the Custom Connector Server Tomcat catalina.log. Determine if the request from the appliance was received.

**Issue:** The list of target applications does not include the custom connectors.

**Actions:**

- Verify that the appliance can communicate with the Custom Connector server. Use the **Test** button on the Configuration, Custom Connector page.
- Examine the PAM Tomcat catalina.log for communication errors, such as timeouts and connection refused
- Look at the Custom Connector Server Tomcat catalina.log. Determine if the request from the appliance was received and is being serviced.

## **Credential Management Issues**

**Issue:** Potential password management problems.

The TCF is tied to the PAM Credential Manager functions. The appliance can try to verify or change passwords using the custom connector. Any issues are recorded in the session logs.

**Action:** Messages in the session logs are labeled to indicate which side of the communication is having a problem:

- Messages that start with **PAM-CF** are appliance-side connector that is related.
- Messages that start with **PAM-EF** are Custom Connector server and TCF related.
- Messages that are from the Custom Connector server itself include address, and possibly a host name

## **Configure SSH Key Pair Policies**

Configure SSH key policies to specify the characteristics that PAM uses to generate SSH key pairs, specifically the cryptographic algorithm to use, and the length of the key.

Use the following procedure to configure PAM SSH key policies for UNIX and Windows SSH Key target connectors.

**Follow these steps:**

1. Select **Credentials, Manage Targets, SSH Key Pair Policies**.
2. Select **Add**.
3. Provide a unique **Name** for the policy.
4. (Optional) Provide a **Description** for the policy.
5. Select the **SSH Key Type**:
  - **UNIX**: ECDSA, RSA, or DSA
  - **Windows SSH Key**: ECDSA or RSA (Windows does not accept DSA keys)
6. Specify the **SSH Key Length**:

- **For ECDSA keys:** 256 bytes, 384 bytes, or 521 bytes
- **For RSA keys:** 1024 bytes, 2048 bytes, or 4096 bytes
- **For DSA keys:** 512 bytes or 1024 bytes

7. Select **OK**.

#### NOTE

For information about target connectors that require SSH key pair policies, see:

- [Add a UNIX Target Connector](#)
- [Add a Windows SSH Key Target Connector](#)

## Add Target Accounts to Target Applications

After you configure a target application and connector, add a target account. The target account identifies an account at the remote server for which PAM can view, and change passwords or certificates.

#### WARNING

Before you add a target account, verify that an account exists on the remote target system. For example, create an Oracle account on the remote Oracle database before you add Oracle as a target account. Make sure that each credential only has one target account.

### Add a Target Account Using the UI

On the **Account** tab, follow these steps to add a target account:


1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. On the **Account** tab, complete the following fields:
  - **Host Name:** Enter the IP address of the remote target system
  - **Device Name:** Enter the name of the remote target system.
  - **Application Name:** Select an existing target application. The application corresponds to an application installed on the remote target server. Complete any additional fields and tabs that might appear.

#### NOTE

For details about target application-specific settings, see [Configure Settings Specific to Individual Target Application Types](#).

- **Account Name:** Assign a *unique* account name for a given account. The account name that you enter must match the account name that is used by the target system. For example, on a UNIX system, account names are the UNIX user ID (userid).

#### NOTE

If the **Provisioned Account** option is set, a search icon (  ) that is used for JIT provisioning appears beside the **Account Name** field.


- **Password View Policy:** The default password view policy is always assigned. Use the magnifying glass to select other defined view policies.
- **Protocol (only for UNIX targets):** This field appears when you select a UNIX target application. From the drop-down list, select the appropriate authentication protocol.

#### NOTE


**SSH-2 Certificate Authentication** cannot be used with the A2A account type.

If you select **SSH-2 Certificate Authentication**, see the [Add the SSH Certificate Target Account and Add Target Accounts to Target Applications](#) section in the [SSH Certificate Authentication for Accessing UNIX/LINUX Targets](#) topic.

If you select **SSH-2 Public Key Authentication**, see the [Add the SSH Key Pair to a Target Account](#) section in the [SSH Key Authentication for Accessing UNIX/LINUX Targets](#) topic.

- **Credential:** The credential of the user account at the remote target server. These credentials must match. Enter a credential or select the **Generate Credential** icon (). The generated credential follows the credential composition policy, and it updates automatically at the target server. For accounts that use the **Generic** application type, manually change the credential on the target system so it matches the one in the secure database.
- **Account Type:** Accept the default, **Privileged Account**, unless you are adding an A2A target. For A2A devices, select **A2A Account**. A2A is only available if your license allows for A2A devices. If you select an SSH certificate authentication for your **Application Name**, this field grays out with a value of Privileged Account. The **Password** and **Compound Servers** tabs also disappear, and the **Certificate** tab appears. See Step 5 for more information on applications that use SSH certificate authentication
- **Access Type (Optional):** The Access type is only for reference. This field is not used by Credential Manager. Use the Access Type value to define dynamic target groups. If you are using target groupings, enter descriptors for the target account.
- **Descriptor 1 and 2 (Optional):** If you are using target groupings, you can enter descriptors for the target account.
- **Provisioned Account (Optional):** Set this option to configure the account as a template for dynamically creating user accounts to support Just in Time (JIT) provisioning.

#### NOTE

Setting the **Provisioned Account** option activates a search icon () beside the **Account Name** field that is used to select an identity template for JIT provisioning.

For more information, see [Create a Target Account for the MSSQL JIT Provisioned Account](#) and [Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account](#).

4. For A2A target accounts, the following fields are optional:
  - **Aliases:** A target alias enables an A2A requestor to request credentials from a specific account without transmitting the account user name and password. Enter a target alias name for the account. The target alias name must be unique across the Credential Manager.
  - **Cache Behavior:** Controls password caching on the A2A Client. Select one of the following options:
    - Use Cache First: The A2A Client looks for the password in the local cache first. If there is no password or if the password is not the most recent, the A2A Client contacts the appliance.
    - Use Server First: The A2A Client contacts the product appliance to get the most recent password. If a password is unavailable, the A2A Client looks in the local cache.
    - No Cache: The password is never stored in the local cache. The A2A Client always contacts the product appliance for the password.
  - **Cache Expiry Days:** Specify how long the password remains in the cache.
5. If you select **SSH-2 Certificate Authentication** for your **Protocol**, the following fields and tabs appear:
  - **Principal:** Optionally, enter a comma-separated list of strings to use as authentication principals. If this field is blank, the **Account Name** is used as a principal. The principals that are defined here should match the principals that are defined on the SSH server.
  - **Certificate Details:** Lists the details of the selected SSH certificate authentication policy that is associated with the target application. For more information about SSH certificate policies, see [Create an SSH Certificate Policy with the UI](#).
  - **Certificates Tab:** This tab appears when you select **SSH-2 Certificate Authentication** for your **Protocol**. This tab displays the following options:
    - **Last Generated:** Displays the most-recent time and date that the certificate was generated. A new certificate is generated and sent to the sshd server on the UNIX system every time a user logs in using MindTerm or an SSH proxy service. **Last Generated** is equivalent to the last time that a user attempted to log in with this target account.
    - **Account Created:** Displays the time and date that the certificate was created.

6. Select **OK**. Your new target account is added to the list of accounts on the Account List page.

### **WARNING**

When you update target account information other than the password, you must manually perform password verification. To verify the password manually, select the **Verify Password** icon on the Account tab for the target account.

### ***Specify AWS Target Account Information***

If the target account is an AWS account, there are more fields that you must configure.

Before doing this procedure, ensure that you have downloaded from AWS the **EC2 Private Key** file. The key file has a `.pem` extension.

### **Follow the steps for adding an AWS target account:**

1. In the **Application Name** field, select **AWS Access Credential Accounts**.  
The Host Name and Device Name fields are populated with the `xceedium.aws.amazon.com` entry.
2. For AWS Access Credential Type, select the **EC2 Private Key** option button.
3. Enter the EC2 Instance User Name, such as `ec2-user` (for Amazon Linux), or `root` (for Red Hat Linux), or other full permission account.
4. Browse and upload the EC2 Private Key file.
5. In Key Pair Name, enter the file name of the EC2 Private Key you uploaded, but without the extension.
6. (Optional) Enter a passphrase to use with the EC2 private key in the Passphrase field.

### **Add a Target Account using the CLI**

To use the CLI, see [Add Target Accounts using the CLI](#).

### **Configure Password Synchronization and Account Discovery**

From the Password tab of a target account, you can view information about a target account password, such as:

Regardless of whether the password has been used, you can also configure account discovery and password synchronization. These two features are documented in the following topics:

- [Account Discovery](#)
- [Password Synchronization](#)

### **Add a Compound Target Account (Optional)**

A compound account consists of several accounts on a cluster of servers, all having the same account name. When the password of a compound account is updated, it is changed on all the cluster members. If the password cannot be changed on all cluster members, roll back the password to the previous value.

The Compound Servers tab shows the status of an update:

- If a password update fails but the subsequent rollback succeeds, the Verified column displays a warning symbol next to the server.
- If a password update fails *and* the subsequent rollback fails, the Verified column displays a red **X** next to the server name. The password on this server is now out of sync.

Compound accounts respect existing target account functions such as, workflow, scheduled jobs, auto-connect, and target group membership.

You can create a compound target account from the Compound Servers tab.

### **NOTE**

You cannot add the host target server as a compound server.

**Follow these steps:**

1. Add a target account or update an existing target account.
2. Select the **Compound Servers** tab.
3. Use the + sign to add servers. The number of servers is not limited, but the recommendation is 20 servers.

**Configure Settings Specific to Individual Target Application Types**

When you add a target account, one or more tabs are added to the Target Account configuration page. The tabs are specific to the target application associated with the target account. Many of these settings are for features unique to one or more target accounts. The following table lists where you can find information about these additional tabs.

For information about target accounts for service desk applications, see [Integrate with Your Service Desk Solution](#).

Application Type for Target Account	UI Setting or Tab	Instructions
Multiple application types	<b>Change Process</b> setting	See <a href="#">Use an Alternate Account to Change Passwords (Optional)</a>
Active Directory	<b>Services</b> and <b>Scheduled Tasks</b> tabs	See <a href="#">Add Services and Scheduled Tasks for Windows Accounts</a>
Cisco	<b>Cisco SSH</b> tab	See <a href="#">Cisco SSH Target Account Configuration</a>
LDAP	<b>DN</b> setting	Enter the distinguished name for the account
MSSQL	<b>MSSQL</b> tab	<a href="#">Configure MSSQL Target Accounts</a>
MSSQL Azure Managed Instance	<b>MSSQL Azure Managed Instance</b> tab	See <a href="#">Configure MSSQL Azure Managed Instance Target Accounts</a>
MYSQL	<b>Database</b> setting	Enter the name of the database on the target system
Oracle	<b>Oracle</b> tab	See <a href="#">Oracle Internet Directory Target Account Settings</a>
Palo Alto	<b>Palo Alto</b> tab	See <a href="#">Palo Alto Account Configuration</a>
SPML v2.0	<b>Database Name</b> setting	Specify the name of the SPML 2.0-compliant database
UNIX	<b>Privilege Elevation</b> setting	See: <a href="#">UNIX Privilege Elevation Setting</a> <a href="#">SSH Access to UNIX Targets</a>
VMware NSX Manager	<b>Access Privileged mode using</b> setting	See <a href="#">Use an Alternate Account to Change Passwords (Optional)</a> The function of this field is the same as the Change Process setting.
Windows SSH Key	Public and private key settings <b>SSH</b> tab	See <a href="#">Add a Windows SSH Key Target Connector</a>
Windows SSH Password	<b>SSH</b> tab	See <a href="#">Add a Windows SSH Password Target Connector</a>
Windows Proxy	Windows Proxy settings	See <a href="#">Register Windows Proxy Target Accounts</a>
Windows Remote	Services and Scheduled Tasks tabs	See <a href="#">Configure Windows Remote Target Accounts</a>



## Add Target Accounts using the CLI

To add a target account using the CLI, use the `updateTargetAccount` commands.

Follow these instructions:

### Encode Complex Passwords with Special Characters

When you define targets (servers, applications, accounts) with the CLI, certain complex passwords, and SSH private keys can be difficult to input with CLI commands. The keys and passwords can contain special characters such as spaces, line feeds, and carriage returns. If the password contains these special characters, the shell (Windows and UNIX) can corrupt the information that Credential Manager receives.

To avoid this issue, perform base-64 encoding on the password *before* adding a target account with the `addTargetAccount` command.

The following utilities can perform base-64 encoding:

- For Windows, use the `b64` utility available at: <http://sourceforge.net/projects/base64/>
- For Linux and UNIX, use the `base64` built-in command.
- For OS X, use the `base64` built-in command.

The following utilities can verify file hashes:

- For Windows, use the Penteract File Checksum Integrity Verifier utility, [available free from Microsoft.](#)
- For Linux, use the `sh1sum` command.
- For OS X, use the `shasum` command.

When you use the `addTargetAccount` command, use the `passwordIsBase64Encoded` parameter and set it to true. If you set this parameter to true, the specified password is Base64-encoded and Credential Manager must decode the password before storing it.

### Add a Target Account with the CLI

This procedure includes the commands for adding all required target objects, that is, a server, an application and an account. For details on the parameters of each command, see [Windows Remote Target Connector CLI Configuration](#) for parameters unique to Windows Remote.

#### 1. Add a target server:

Windows:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 ^
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

Linux:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 \
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

#### 2. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetServer>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
```



```

<ID>1</ID>
<createDate>Mon Nov 12 15:35:14 EST 2007</createDate>
<updateDate>Mon Nov 12 15:35:14 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>XhMAD33ITheWuMB1L89Zsxfdxsg=</hash>
<hostName>Vienna-Lab3.cloakware.com</hostName>
<IPAddress>11.1.0.3</IPAddress>
</TargetServer>
</cr.result>
</CommandResult>

```

### 3. Add a target application:

#### Windows:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetApplication ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.type=Generic ^
TargetApplication.name='Generic Application Type' Attribute.descriptor1=Vienna ^
Attribute.descriptor2=Lab

```

#### Linux:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetApplication \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.type=Generic \
TargetApplication.name='Generic Application Type' Attribute.descriptor1=Vienna \
Attribute.descriptor2=Lab

```

### 4. Enter your password at the prompt. Credential Manager returns the following XML command string.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetApplication>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:38:32 EST 2007</createDate>
<updateDate>Mon Nov 12 15:38:32 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>kvSzMfnFi2iCIihAVt85+N2jzpc=</hash>
<targetServerID>1</targetServerID>
<type>Generic</type>
<name>Generic</name>
<policyID>0</policyID>
</TargetApplication>
</cr.result>
</CommandResult>

```

### 5. Add a target account:

#### Windows:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAccount ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.name='Generic Application Type' ^
TargetAccount.userName=account1 TargetAccount.password=123456 ^
passwordIsBase64Encoded=true TargetAccount.cacheBehavior=useCacheFirst TargetAccount.privileged=false ^
TargetAccount.cacheDuration=20 TargetAccount.accessType='A generic system account' ^

```

```
TargetAccount.synchronize=false Attribute.changePasswordAfterViewing=true ^
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

**Linux:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAccount \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.name='Generic Application Type' \
TargetAccount.userName=account1 TargetAccount.password=123456 \
passwordIsBase64Encoded=true TargetAccount.cacheBehavior=useCacheFirst TargetAccount.privileged=false \
TargetAccount.cacheDuration=20 TargetAccount.accessType='A generic system account' \
TargetAccount.synchronize=false Attribute.changePasswordAfterViewing=true \
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

**6. Enter your password at the prompt. Credential Manager returns the following XML command string.**

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true
</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 EST 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>l4adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheBehavior>useCacheFirst</cacheBehavior>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>
</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>
```

**7. If the account type is A2A (only possible if your license allows for A2A accounts), add a target alias:****Windows:**

```
Windows:
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAlias ^
TargetAlias.name=ViennaAlias5 TargetServer.hostName=Vienna-Lab3.cloakware.com ^
TargetApplication.name='Generic Application Type' TargetAccount.userName=account1
```

**Linux:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAlias \
TargetAlias.name=ViennaAlias5 TargetServer.hostName=Vienna-Lab3.cloakware.com \
```

```
TargetApplication.name='Generic Application Type' TargetAccount.userName=account1
```

**8. Enter your password at the prompt. Credential Manager returns the following XML command string.**

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAlias>
<ID>1</ID>
<createDate>Mon Nov 12 15:43:24 EST 2007</createDate>
<updateDate>Mon Nov 12 15:43:24 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>iB6pR3X7E8yP8p4RemqsChneEQc=</hash>
<name>ViennaAlias5</name>
<accountID>1</accountID>
</TargetAlias>
</cr.result>
</CommandResult>
```

### **Add a Compound Account (Optional)**

To add multiple servers that have the same account, you can specify compound servers.

**Follow these steps:**

1. Add a target server as shown in the previous example in this topic
2. Enter your password at the prompt.
3. Add one or more servers:

**Windows:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 ^
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

**Linux:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetServer \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetServer.ipAddress=11.1.0.3 \
Attribute.descriptor1=Vienna Attribute.descriptor2=Lab
```

**4. Enter your password at the prompt. Credential Manager returns the following XML command string.**

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetServer>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>2</ID>
<createDate>Mon Nov 12 15:35:14 EST 2007</createDate>
<updateDate>Mon Nov 12 15:35:14 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>XhMAD33ITheWuMB1L89Zsxfdxsg=</hash>
<hostName>Vienna-Lab3.cloakware.com</hostName>
```

```
<IPAddress>11.1.0.4</IPAddress>
</TargetServer>
</cr.result>
</CommandResult>
```

Repeat step 3 and 4 for each compound server you want to add. Each `addTargetServer` operation returns a new ID value.

5. Add a target application as shown in the previous example in this topic.
6. Enter your password at the prompt.
7. Add a compound target account:

For the `TargetAccount.compoundServerIDs` parameter, list each `<ID>` value that is returned in steps 3 and 4, separated by commas.

**Windows:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAccount ^
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.name='Generic Application Type' ^
TargetAccount.userName=account1 TargetAccount.password=123456 ^
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.privileged=false ^
TargetAccount.cacheDuration=20 TargetAccount.accessType='A generic system account' ^
TargetAccount.synchronize=false Attribute.changePasswordAfterViewing=true ^
TargetAccount.isCompound=true TargetAccount.compoundServerIDs=1,2 Attribute.descriptor1=Vienna ^
Attribute.descriptor2=Lab
```

**Linux:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addTargetAccount \
TargetServer.hostName=Vienna-Lab3.cloakware.com TargetApplication.name='Generic Application Type' \
TargetAccount.userName=account1 TargetAccount.password=123456 \
TargetAccount.cacheBehavior=useCacheFirst TargetAccount.privileged=false \
TargetAccount.cacheDuration=20 TargetAccount.accessType='A generic system account' \
TargetAccount.synchronize=false Attribute.changePasswordAfterViewing=true \
TargetAccount.isCompound=true TargetAccount.compoundServerIDs=1,2 Attribute.descriptor1=Vienna \
Attribute.descriptor2=Lab
```

8. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true
</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 EST 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>14adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
```

```

<cacheBehavior>useCacheFirst</cacheBehavior>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>
</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>

```

## Use Account Discovery to Add Target Accounts

A subset of out-of-the-box target applications offers the Account Discovery feature. Account Discovery is a mechanism to add target accounts easily. You can use it as an alternative to manually adding target accounts.

The following application types offer Account Discovery:

- [UNIX/LINUX](#)
- [Active Directory](#)
- [LDAP](#)
- [Windows Remote](#)
- [Windows Proxy](#)

### NOTE

If you discover accounts using Amazon AWS integration, the **Address** field of the device must include the fully qualified domain name or IP address. If a device using AWS integration has already been discovered, recreate the device.

### Account Discovery Prerequisites

Before you can use Account Discovery, you must configure the targets that the appliance searches for discovery. For any managed target, configure the following items:

1. Target servers. See [Device Discovery](#).
2. Target Applications. Configure one of the target applications that support Account Discovery.
3. Target Accounts for each target application that supports Account Discovery.

When you add a target account, the **Discovery Allowed** option is available. Selecting this option indicates that the account is available for discovery. Select this option only for accounts that you want to scan for discovery.

### NOTE

You can use an account to scan only for other accounts that support the same target application. For example, use a Windows domain account that is configured with an Active Directory target application to scan for other accounts that use the Active Directory application type. You cannot use the Windows domain account to scan for local accounts that are configured with a Windows Proxy target application.

For UNIX accounts, selecting Discovery Allowed also adds the checkbox **Allow multiple server discovery for this type of application**. This checkbox indicates that the account is a discovery account for any server and application of this type. For example, if you have 20 servers with a common account and password, use one account and select this box. Then for any discovery job with this application type selected, this account is used as a credential for discovery.

## Discover Accounts Using a Scan

To discover accounts, follow these steps:

1. Go to **Credentials, Discovery**.
2. Select **Discovery** from the Targets Menu.
3. Create a Scan Profile:
  - a. From the Scan Profiles tab, select **Add**.
  - b. On the Profile tab, complete the fields.
  - c. On the Servers tab, move Available Servers to Selected Servers with the arrow button. The listed available servers are managed devices.
  - d. The Purge Interval field sets the number of days that discovered devices are deleted, unless the devices are discovered by another profile. The Purge Interval default is set on the Global Settings page, under Basic Settings, as Scan Purge Interval.
4. Run the scan.
  - a. Create a schedule to run the scan or run it on demand.
    - Use the Schedule tab to create an optional schedule. Once you select a frequency, other fields appear. Select the appropriate time intervals. Select OK to save the Scan Profile.
    - To run the scan on demand rather than on a schedule, select OK to save it. Select the Scan Profile from the Scan Profiles list, and select the Run button above the list.
  - b. Once a scan is running, monitor its progress on the Scan Profile Jobs tab. You can also cancel the job on this panel by selecting Cancel Job. Once it is complete, view a summary of its results on the Scan Profile History tab. The Scan Profile Jobs and other tables are refreshed according to the default setting on the Global Settings page. Table Refresh Interval is in the Basic Settings section, and defaults to 60 seconds.

### NOTE

Selecting **Delete** for a highlighted profile deletes its Scan Profile History. **Delete** also deletes any Accounts that are associated with that Profile unless they are associated with another Profile.

After a scan is complete, you can:

- [View the scan results](#)
- [Export results to a CSV file](#)
- [Bring discovered accounts under management.](#)
- [Update discovered accounts.](#)

## View the Scan Results

Select the Scan Profile History tab to view the results of the account discovery scans. Each row shows a Scan Profile, its latest Discovery time, and a summary of the scan results. The summary shows a count of discovered accounts, how many are new, and not found. "Not found" Accounts were discovered by a previous run of the same Scan Profile, but are now missing. The Summary shows the same information about SSH Keys. See [SSH Key Discovery](#) for more information. The Summary also shows a count of any errors that were encountered. These numbers refer only to the latest run of this scan profile.

Use the **Filter** button to filter the display on the page. You can use asterisks and percent signs as multiple-character wildcards.

### View Summary Details

The View Summary Details button opens the Scan Results window. The Scan Information tab displays the Scan Profile name and the Job Time. The Discovered Accounts, New Accounts, and Not Found Accounts tabs list the Account Names in each respective category. For information about the Discovered Keys, New Keys, and Not Found Keys, see [SSH Key Discovery](#). The Logs tab displays a table including each action that is taken regarding this scan.

To see all scans that have run for a given Profile, select the View Scans button above the Summary. Clicking the Summary numbers lists the accounts or keys that are discovered in the same panel as View Summary Details. You can also select the View Summary Details button to get to this panel.

### **View Account Scan Results**

To see information about the discovered accounts, go to the Scan Profile History panel and select **Scan Profile, View Account Scan Results**. The account name, the device where it was found, the application, and a timestamp are displayed. A checkbox indicates whether Credential Manager manages the account.

On the history panel, are the following controls:

- **Filter:** Filter the display on the page by column values. You can use asterisks and percent signs as multiple-character wildcards.
- **Export:** Create a CSV file with a row for each Discovered Account listed.
- **View:** Show the data for one row whose Account Name box is checked. In the Logs tab, it displays log information that is not shown in the Account Scan results panel.
- **Manage:** Bring an account under management. To manage accounts, select one or more accounts names. Then select **Manage**. The Manage Discovered Accounts window opens.

### **View All Scans**

To see all discovered accounts rather than only the accounts for a given scan, select the **Discovered Accounts** tab. The displayed table lists each Account Name, Device Name, Application Name, Latest Discovery Time, and whether it Is Managed.

On this tab are the following controls:

- **Filter:** Filter the display on the page by column values. You can use asterisks and percent signs as multiple-character wildcards.
- **Export:** Create a CSV file with a row for each Discovered Account listed.
- **View:** Show the data for one row whose Account Name box is checked. In the Logs tab, it displays log information that is not shown in the Account Scan results panel.
- **Manage:** Bring an account under management. To manage accounts, select one or more account names then select **Manage**. The Manage Discovered Accounts window opens.

### **Bring Discovered Accounts Under Management**

To manage an account from the Discovered Accounts window, follow these steps:

1. From the Discovered Accounts tab, select **Manage**. The Manage Discovered Accounts window opens.
2. Select a synchronization option. This option is not available if the application type is **Generic**.
  - **Update only the Password Authority Server.** Passwords are only updated in Credential Manager. Credential Manager and target system passwords can differ.
  - **Update both the Password Authority Server and the target system.** Password updates are performed in both Credential Manager and the target system to maintain consistency.

#### **NOTE**

For the Windows Proxy and Windows Remote application types, the discovered accounts have the **Force password change** option enabled automatically.

3. For most target account types, a **Password Change Process** option is available. This option lets you select whether the managed account can change its own password or whether another, higher-privilege account must do that. If you select **Use the following account to change the password**, a field appears below the legend so that you can select the password-changing account.

Some application types allow an account password to be updated from another account (for example, root). If this situation applies, select that account. The account that is used to change the password must already be registered in Credential Manager.

4. To generate a random password for each account, select the **Generate credential for each account** checkbox.
5. Select whether the account type is Privileged Account or an A2A account (A2A is available only with a license). If you select A2A, more fields appear. You can set the Cache Behavior to use the Cache or the Server first, or not use a cache. You can also set the Cache Expiry in days.
6. **Password View Policy** allows you to select a policy, including a Default policy. Access Password View Policies from the Workflow menu.
7. Enter a **Password**. The Account Details page (Accounts option on the Targets menu) has more options that are not presented here. Once an Account is managed, you can access it from the Accounts page.
8. (Optional) For or customer convenience, enter a value for the **Access Type** to define dynamic target groups. This field is only for reference and is not used by Credential Manager.
9. (Optional) If you are using target groupings, enter **Descriptors**.
10. Select **OK** to save.

### **Update Discovered Accounts (Windows Proxy or Windows Remote Accounts Only)**

To add new tasks and services to Windows Proxy or Windows Remote Accounts, follow these steps:

1. Select **Credentials, Discovery**.
2. On the Scan Profiles tab, select **Run** for the Profile with the account you want to update. If a Profile does not exist, select **Add**. Give it a **Name**. On the Servers tab, select the Server that is associated with the Proxy or Remote Account. Select **Run**.
3. Select the **Discovered Accounts** tab.  
Windows Proxy or Windows Remote accounts that have updates available display a green checkbox under the Updates Available column.
4. Select the **Update** button for the Windows Proxy or Windows Remote account with updates available.  
The Update Discovered Accounts windows appears. Available Services and Scheduled Tasks appear on their respective tabs.
5. Select **OK**.
6. Select **Yes** when you are prompted to Update Selected Accounts.  
The managed Services and Scheduled Tasks appear on their tabs on the Account, under Credentials, Manage Targets, Accounts.

To remove tasks and services from Windows Proxy or Windows Remote Target Accounts, follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the account that you want to modify.
3. Select **Update**.
4. Select the Services or Tasks tab.
5. Select the service or task you want to delete. Select the **Delete** icon.

#### **NOTE**

- Discover Linux or UNIX SSH keys for auditing: See [SSH Key Discovery](#) for more information.
- Discover Windows services and scheduled tasks for AD accounts: See [Discover Services and Scheduled Tasks for AD Accounts](#).

## **Synchronize Target Account Passwords**

Synchronization ensures that password updates that are made in the Credential Manager database are also made to passwords stored at the remote target system. When passwords are synchronized, the appliance pulls credentials from



the Credential Manager database and then it sends the credentials to the target system. The target system then verifies whether the credentials are accurate.

#### NOTE

Password synchronization needs an associated [password composition policy](#). When Credential Manager generates a password, it meets the criteria of the composition policy.

You can synchronize passwords for individual accounts and for a group of target accounts. For compound account groups, synchronization updates a series of replicated databases with the same password and keeps the passwords that are synchronized with each other.

You can configure password updates at the following times:

- Immediately
- After a password is viewed
- When it attains a certain age
- On a configured schedule

There is no limit to how many previous passwords PAM stores or to how long passwords are kept.

### **Enable Password Synchronization**

When you add a target account or you update an existing account, you can enable password synchronization.

#### **Follow these steps:**

1. In the UI, go to **Credentials, Manage Targets, Accounts**.
2. Select **Add** or double-click an account in the Target Accounts list.
3. Select the **Password** tab.
4. For the **Synchronized** option, select the behavior that you want between the Credential Manager database and the target system:
  - Update only the Credential Manager Server. This option allows the PAM and target system passwords to differ.
  - Update both the Credential Manager Server and the target system

#### NOTE

Synchronization is not available for accounts that use the Generic application type.

5. In the **Owner User Name** field, select the Credential Manager user
6. Select **OK**.

If a target account is a Windows Proxy account, Credential Manager directs the Windows Proxy to verify the password and update it.

To learn more about password synchronization, review the following topics:

- [Verify Synchronized Target Account Passwords](#)
- [Schedule Password Updates and Verifications](#)

### **Verify Synchronized Target Account Passwords**

On the Target Accounts page (**Credentials, Manage Targets, Accounts**), accounts are displayed with many details, including whether they are verified. The **Verified** column displays only when synchronization is enabled.

Some operations, such as Account Discovery, require an account to be verified.

#### **Verify Account Passwords using the UI**

Use the following procedure to verify a synchronized target account password from the UI.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. A list of target accounts appears.
2. Double-click the target account whose password you want to verify.
3. Select the Verify Credential icon (a blue person with green checkmark), located to the right of the Password field. A message indicating successful password verification appears.

**Verify Account Passwords using the CLI**

To verify synchronized target account passwords with the CLI, use the `verifyAccountPassword` command.

**Follow these steps:**

1. Search target accounts to retrieve the target account ID:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount
TargetAccount.userName=account1
```

2. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1233</ID>
<createDate>Mon Nov 12 15:42:43 EST 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>14adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>Mon Nov 12 15:42:43 EST 2007</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>
```

3. Run the following command:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=verifyAccountPassword TargetAccount.ID=1233
```

4. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
```

```

<TargetAccount>
<privileged>true</privileged>
<aliases></aliases>
<password>{1}8ae8e633c1fa6020bfb7695e17f83f18</password>
<lastUsed></lastUsed>
<passwordViewPolicyID>1000</passwordViewPolicyID>
<targetApplicationID>1222</targetApplicationID>
<userName>sqlaccount1</userName>
<accessType></accessType>
<cacheDuration>30</cacheDuration>
<synchronize>true</synchronize>
<cacheBehavior>useCacheFirst</cacheBehavior>
<lastVerified>Tue Apr 05 11:47:40 UTC 2011</lastVerifi
ed><lastViewed></lastViewed>
<passwordVerified>true</passwordVerified>
<compoundAccount>false</compoundAccount>
<targetApplication></targetApplication>
<cacheAllow>true</cacheAllow>
<targetServerAlias></targetServerAlias>
<ID>1233</ID>
<Attribute.extensionType>mssql</Attribute.extensionType>
<Attribute.useOtherAccountToChangePassword>false</Attribute.useOtherAccountToChangePassword>
<Attribute.cspm_serverkeyid>1</Attribute.cspm_serverkeyid><Attribute.descriptor1></Attribute.descriptor1>
<Attribute.descriptor2></Attribute.descriptor2>
<createDate>Tue Apr 05 11:44:37 UTC 2011</createDate><extensionType>mssql</extensionType>
<updateUser>admin</updateUser><updateDate>Tue Apr 05 11:47:40 UTC 2011</updateDate>
<createUser>admin</createUser><hash>EuufPEVlFusXtH6XF3rs7BbEJFY=</hash>
</TargetAccount>
</cr.result>
</CommandResult>

```

If the password is not verified, the attribute `passwordVerified` returns a "false" value; for example, `<passwordVerified>false</passwordVerified>`.

## Schedule Password Updates and Verifications

For synchronized target accounts, you can schedule:

- Regular password updates: Scheduled password updates use automatically generated passwords that conform to your specified password composition policies. If the passwords in the appliance database and at the remote target match, the scheduled job updates both passwords.
- Password verifications: Verifications ensure whether passwords are in sync.

For password updates or verifications, you can schedule jobs on a per account basis or per target group basis. When a job is scheduled for a group, the appliance performs the update or verification on each synchronized target accounts in that group. If a single update or verification fails, the job status is marked as failed. However, the job continues to process the remaining updates or verifications.

This topic explains how to:

### Schedule an Update or Verification

Follow these steps:

1. Select **Credential, Manage Targets, Scheduled Jobs**.

2. Select **Add**.  
The Add Scheduled Job page appears.
3. Enter the **Job Name**. Use a text description for the job, up to 80 characters long.
4. In the **Recurrence** field, select the frequency. You can select **Run Once**, **Daily**, **Weekly**, **Monthly**, **Yearly**, and **Every N Days**.
5. The **Date/Time** option changes to correspond with your **Recurrence** selection:
  - a. For **Run Once**, use the **Date/Time** option to select the date and time to run one instance.
  - b. For **Daily**, use the **Time** option to select the time to run a daily instance. The **Repeat Only On Weekdays** option excludes a daily run on any weekend day (Saturday and Sunday).
  - c. For **Weekly**, use the **Time** option to select the time and the days of the week to run the instance.
  - d. For **Monthly**, you have two options:
    - **Run on day <number> of the selected month(s)**: Select a date (1 to 31), or **Last** for the last day of the month to run the job. You can select one or more months to run the job using the corresponding checkbox beneath this option.
    - **Run on the <number><day> of the selected month(s)**: Select First, Second, Third, Fourth, or Last day to run the job. This option allows you to specify a particular day instead of a particular date. You can select one or more days and months to run the job.
  - e. For **Yearly**, use the **Date/Time** option to select the date and time to run the annual instance.
  - f. For **Every N Days**, use the **Date/Time** option to select the start date and time, and then how long to wait before running another instance. For example, you could select a start date, and set the time to 1 AM every four days, by setting the **Time** to 01:00:00 and the **Days** to 4.
6. On the **Account Details** tab, select one of the following entries from the **Command** drop-down list:
  - **Update Target Account Password** for password updates
  - **Verify Account Password** for password verification.
7. Select whether you want this job to apply to a target group or individual account.
8. Specify either the target group or individual target account for this job.

#### NOTE

Account updates or verifications proceed sequentially within a job. However, scheduled jobs can run concurrently. Therefore, having more jobs that are shorter performs better and faster than having fewer jobs that are long.

9. For the "Update Target Account Password" command:
  - Select whether Credential Manager generates the new password. If you select No, extra fields appear so you can supply the new password.
  - For Credential Manager generated passwords, select whether to apply the same new password to all accounts in the group.
10. Select **OK**.

### View the Progress of Scheduled Jobs

To view the status of scheduled jobs, generate the Scheduled Jobs Report. See [Generating Reports](#).

## Use an Alternate Account to Change Passwords (Optional)

For specific application types, Credential Manager can use an alternate master account with sufficient privileges to update a specific target account password. When a user does not have permission to change their own passwords, this alternate account lets Credential Manager synchronize user accounts. If a user changes a password on the target system, Credential Manager can use the master account to override the change and update the password.

When you add a target account, a tab for the associated application type becomes available. On that application tab, there is a **Change Process** setting. The following page is an example for an LDAP application type:

To allow the existing target account to change its own password, keep the default option, **Account can change own password**, selected. The initial password that you enter must be the same as the target account password. The exception is a user with more privileges, such as root, who can update the password.

To use an alternate master account:

1. Select **Use the following account to change password**. For most target accounts, a blank field appears below the radio button.
2. Select the magnifying glass and search for the target account to use as the alternate. Avoid using the current target account as the alternate.  
To show the target accounts that are defined in the system, filter by account name or host name. You can also show all target accounts. Typically, the other account is an account of the same application. For example, the password for an Oracle database account is changed by a privileged account on the same database. You can use another account that is associated with a different application. Select compatible combinations.

#### NOTE

The only supported dissimilar account combination is the use of an LDAP or Active Directory account to change the password of a UNIX account.

3. Some target accounts require additional information:  
MYSQL: Identify the account by specifying the user name and the hostname of the database. Enter the hostname in the **host-Name Qualifier** field.

## Configure Windows Remote Target Accounts

This section describes the configuration steps for Windows Remote target accounts.

### Prerequisites for Windows Remote Target Accounts

To configure Windows Remote target accounts, including Windows services, ensure that the following tasks are completed:

- Add a device (target server) with Password Management as the device type.

#### NOTE

If you are adding an AWS Windows device, use the private IP address in the Address field of the account. Some features do not function properly when you use the public IP address.

- Add a target application for the target server. This step includes associating Windows Remote with the host on which the Windows account resides. See [Add a Windows Remote Target Connector](#).
- If the Windows Remote target account is of the Administrator account type, the account requires Administrator rights on the Windows server.

#### NOTE

If your target account is to be used as a service account (that is, it is to be used to rotate passwords of other target accounts), we recommend that you prevent this account from being able to log in interactively. To do this, assign the following User Rights to the Windows account:

- **Deny log on locally**
- **Deny log on through Remote Desktop Service**
- If the Windows Remote target account is a domain account, log in to the target system using that account. Logging in establishes the Windows user environment for the domain account, which is required for the Windows remote target connector to function.

### **Create a Windows Remote Target Account**

Use this procedure to create a Windows Remote target account using the PAM UI.

To add a Windows Remote Target account using the CLI, see [Windows Remote Target Connector CLI Configuration](#).

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. The Target Account page appears with a list of existing accounts.
2. Select **Add**. The Add Target Account page appears.
3. Select the **Host Name** magnifying glass to find an existing target server, filling the Host Name and **Device Name**.
4. Select the **Application Name** magnifying glass to find an existing target application on the target server, or select **+** to create a target application. Select or create a Windows Remote type of target application. The Windows Remote appears on the Add Target Account page.
5. Enter the **Account Name**. The account name must be unique for a given target application and must be the account name that the target system uses.
6. Select the **Password View Policy** for the account.
7. Enter an initial account **Password** or select the Generate Credential key icon to generate a default password.
8. On the **Password** tab, Select **Discovery Allowed** to discover accounts on the Windows remote system. Select the appropriate synchronization option:
  - Update only the Credential Manager Server: Passwords are updated only in Credential Manager. Credential Manager and target system passwords can differ.
  - Update both the Credential Manager Server and the target system: Password updates are performed both in Credential Manager and on the target system to maintain consistency.
9. On the **Windows Remote** tab, select the **Account Type**:
  - User: If you select a regular User account, select "Use the following account to change password" for the **Change Process**.
  - Administrator: If you select Administrator, use either **Change Process** option.
10. If you select the magnifying glass next to "Use the following account to change password" for the **Change Process**, a Target Account dialog appears. Select an account that is of Administrator account type from the same Windows Remote application.
11. (Optional) If you are adding or updating an account and you do not know the existing password, select the **Force password change** checkbox. The existing password gets changed, even though the account is not in sync.
12. Select **OK** to save.  
Your new Windows target account is added to the list of accounts on the Target Accounts page.

### **Discover Windows Services and Scheduled Tasks**

You can use account discovery to manage the credentials of multiple Windows services and scheduled tasks. PAM can use the target account to manage changes and updates for any services and scheduled tasks that use this account. You do not have to update the password on an individual service or scheduled task basis.

#### **NOTE**

This procedure is for local Windows accounts. To discover services and scheduled tasks for Active Directory accounts, see [Discover Services and Scheduled Tasks for AD Accounts](#).

#### **Prerequisite**

Before you run account discovery, go to the Account Discovery tab of the Windows Remote Target application. Select the discover option for services or tasks. You can select both.

### **Discover Services and Tasks**

To discover new tasks and services on Windows remote accounts, follow these steps:

1. Select **Credentials, Discovery**.
2. On the Scan Profiles tab, select **Run** for the profile of the account you want to update.  
If a profile does not exist, follow these steps:
  - a. Select **Add**.
  - b. Give the profile a **Name**.
  - c. On the Servers tab, select the Server that is associated with the remote account.
  - d. Select **Run**.
3. Select the **Discovered Accounts** tab.  
Windows Remote accounts that have updates available display a green checkbox under the Updates Available column.
4. Select the **Update** button for the Windows Remote account with updates available.  
The Update Discovered Accounts window appears. Available Services and Scheduled Tasks appear on their respective tabs.
5. Select **OK**.
6. Select **Yes** when you are prompted to Update Selected Accounts.
7. To see a list of services and scheduled tasks:
  - a. Select **Credentials, Manage Targets, Accounts**.
  - b. Select the Services and Scheduled Tasks tabs to display the list of accounts.

To remove tasks and services from a Windows Remote Target Accounts, follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the account that you want to modify.
3. Select **Update**.
4. Select the Services or Scheduled Tasks tab.
5. To delete a service or task, select the **X** next to the entry.

#### **NOTE**

**More Info:** [Use Account Discovery to Add Target Accounts](#)

## **Configure MSSQL Target Accounts**

This topic describes how to configure MSSQL target accounts.

### **Follow these steps:**

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.
3. Complete the following fields on the **Account** tab of the **Add Target Account** pane that opens:
  - **Host Name:** The IP address or FQDN of the MSSQL host.
  - **Device Name:** The name of the MSSQL device.
  - **Application Name:** The name of the MSSQL target application.
  - **Account Name:** Assign a *unique* account name for each account. The account name that you enter must match the account name that is used by the target system. For example, on a UNIX system, account names are the UNIX user ID (userid).

**NOTE**

If the **Provisioned Account** option is set, you can use the search icon (🔍) that appears to specify the account name from the **Extended Identity Templates** dialog that opens. For more information, see [Create a Target Account for the MSSQL JIT Provisioned Account](#).

- **Password View Policy:** The name of the password view policy that you created for the account.
- **Password:** Any text that matches the password composition policy for the target account (provisioned account passwords are not managed within PAM).
- **Provisioned Account** (Optional): Set this option to configure the target account as a template for dynamically creating user accounts to support MSSQL Just in Time (JIT) provisioning.

**NOTE**

Setting the **Provisioned Account** option activates a search icon (🔍) beside the **Account Name** field that is required to select an identity template for JIT provisioning.

For more information, see [Create a Target Account for the MSSQL JIT Provisioned Account](#).

4. On the **MSSQL** tab, select one of the following options and complete any associated configuration:
  - **Account can change own password**
  - **Use the following account to administer changes**

Complete the following steps to select the account to use to administer changes

  1. Select the Search icon (🔍) beside the text field that appears.
  2. Choose the required account from the **Target Accounts** dialog that opens as shown in the following example

**Target Accounts**

Column: 

Application Type

Value: 

MSSQL

Account Name	Application Name	Application	Host Name	Device Nam	Account Ty	Owner User	Verified
\${User.userPrincipalName}	MSSQL JIT	MSSQL	10.252.5...	MSSQL	Privileged		
sa	MSSQL DB	MSSQL	10.252.5...	MSSQL	Privileged		<div></div>

screenshot:

**NOTE**

When a user performs checkout and check-in operations using a provisioned account, their account name is replaced with the RDP User Name set in the User Information (Provisioned Account, *MYLDAP\TestUser1*) on the **Access** page.

3. Select **OK**.

## Configure MSSQL Azure Managed Instance Target Accounts

This topic describes how to configure MSSQL Azure Managed Instance target accounts for Azure SQL Managed Instances.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.
3. Complete the following fields on the **Account** tab of the **Add Target Account** pane that opens:



- **Host Name:** The IP address or FQDN of the Azure SQL managed instance.
- **Device Name:** The name of the Azure SQL managed instance.
- **Application Name:** The name of the Azure SQL Managed Instance target application.
- **Account Name:** Assign a *unique* account name for each account. The account name that you enter must match the account name that is used by the target system. For example, on a UNIX system, account names are the UNIX user ID (userid).

**NOTE**

If the **Provisioned Account** option is set, you can use the search icon (🔍) that appears to specify the account name from the **Extended Identity Templates** dialog that opens. For more information, see [Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account](#).

- **Password View Policy:** The name of the password view policy that you created for the provisioned account.
- **Password:** Any text that matches the password composition policy for the target account (provisioned account passwords are not managed within PAM).
- **Provisioned Account** (Optional): Set this option to configure the target account as a template for dynamically creating user accounts to support Azure SQL Managed Instance Just in Time (JIT) provisioning.

**NOTE**

Setting the **Provisioned Account** option activates a search icon (🔍) beside the **Account Name** field that is used to select an identity template for JIT provisioning.

For more information, see [Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account](#).

4. On the **MSSQL Azure Managed Instance** tab, select one of the following options and complete any associated configuration:
  - **Account can change own password**
  - **Use the following account to administer changes**

Complete the following steps to select the account to use to administer changes

1. Select the Search icon (🔍) beside the text field that appears.
2. Choose the required account from the **Target Accounts** dialog that opens as shown in the following example

### Target Accounts


Column:	Application Type	Value:	MSSQL Azure Manager				
Account N	Application Name	Application Type	Host	Device Na	Account T	Owner Use	Verifie
sa	Azure SQL MI DB	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		✓
\${User...	Azure SQL MI JIT	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		
\${User...	Azure SQL MI JIT	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		

screenshot:

OK

Cancel

**TIP**

- Accounts from the Azure SQL Managed Instance have an Application Type of "MSSQL Azure Managed Instance" and are listed by default.
- Accounts from an Azure AD have an Application Type of "Azure Access Credentials." To view such accounts, change the selection filter value to "Azure Access Credentials."
- To list all accounts, select the **Reset** icon (  ).

3. Select **OK**.

## Configure IBM i Target Accounts

This section describes the configuration steps for IBM i (formerly AS/400) target accounts.

### Prerequisites for IBM i Target Accounts

To configure IBM i target accounts, ensure that the following tasks are completed:

- Add a device (target server) with Password Management as the device type.

**NOTE**

If you are adding an AWS IBM i device, use the private IP address in the Address field of the account. Some features do not function properly when you use the public IP address.

- Add a target application for the target server. This step includes associating IBM i with the host on which the account resides. See [Add an IBM i Target Connector](#).

To add an IBM i Target account using the CLI, see [IBM i Target Connector CLI Configuration](#).

### Create an IBM i Target Account

Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**. The Target Account page appears with a list of existing accounts.
2. Select **Add**. The Add Target Account page appears.
3. Select the **Host Name** magnifying glass to find an existing target server, filling the Host Name and **Device Name**.
4. Select the **Application Name** magnifying glass to find an existing target application on the target server, or select **+** to create a target application. Select or create an IBM i type of target application.  
The IBM i appears on the Add Target Account page.
5. Enter the **Account Name**. The account name must be unique for a given target application and must be the account name that the target system uses.
6. Select the **Password View Policy** for the account.
7. Enter an initial account **Password** or select the Generate Credential key icon to generate a default password.
8. On the **Password** tab, Select **Discovery Allowed** to discover accounts on the IBM i system. Select the appropriate synchronization option:
  - Update only the Credential Manager Server: Passwords are updated only in Credential Manager. Credential Manager and target system passwords can differ.
  - Update both the Credential Manager Server and the target system: Password updates are performed both in Credential Manager and on the target system to maintain consistency.
9. On the **IBM i** tab, do the following steps:
  - a. Select the **Account Type**:
    - **User**: Use a regular user account.
    - **Administrator**: Use an administrator account.
  - b. Select the Change Process:

- If you selected **User** as your **Account Type**, select **Use the following account to change password** and type the name of or use the magnifying glass icon to specify an account that is of the Administrator account type for the same IBM i application.
- If you selected **Administrator** as your **Account Type**, use either **Change Process** option.
- (Optional) If you are adding or updating an account and you do not know the existing password, select the **Force password change** checkbox. The existing password gets changed, even though the account is not in sync.

c. Select **OK** to save.

Your new IBM i target account is added to the list of accounts on the Target Accounts page.

### **Configure PAM to Allow Non-Administrative Users to Unlock IBM i Target Accounts Without Administrative Privileges.**

#### **WARNING**

This feature provides self-service password unlock for privileged users who are inadvertently locked out of an account whose password they have permission to view. However, we strongly recommend that administrators that provision privileged account access consider the security and compliance policy implications of configuring this functionality. Self-service unlock events are included in the session log for auditing purposes.

This procedure describes how to configure PAM to enable local non-administrative user to unlock an IBM i target account that has been locked for some reason, such as in the following example scenario:

1. A user logs into PAM and accesses a target account for an IBM i system and checks out the credentials. The target account is assigned a password view policy with the following options set:
  - Check-out / Check-in
  - Change Password on View
2. Later on, the user attempts to login to the IBM i system from an external terminal emulator using the password they checked out earlier but it is no longer valid for one of the following reasons:
  - The **Force check-in after** period configured in the password view policy has expired and the password has been rotated
  - A local administrator has changed the password on the IBM i system.
3. The user reattempts to use the password until they exceed the maximum number of allowed failed login attempts configured on the IBM i system and the account is locked.

### **Discover IBM i Services and Scheduled Tasks**

You can use account discovery to manage credentials of multiple IBM i services and scheduled tasks. PAM can use the target account to manage changes and updates for any services and scheduled tasks that use this account. You do not have to update the password on an individual service or scheduled task basis.

#### **NOTE**

This procedure is for local IBM i accounts. To discover services and scheduled tasks for Active Directory accounts, see [Discover Services and Scheduled Tasks for AD Accounts](#).

#### ***Prerequisite***

Before you run account discovery, go to the Account Discovery tab of the IBM i Target application. Select the discover option for services or tasks. You can select both.

#### ***Discover Services and Tasks***

To discover new tasks and services on IBM i accounts, follow these steps:

1. Select **Credentials, Discovery**.
2. On the Scan Profiles tab, select **Run** for the profile of the account you want to update.

If a profile does not exist, follow these steps:

- a. Select **Add**.
- b. Give the profile a **Name**.
- c. On the Servers tab, select the Server that is associated with the remote account.
- d. Select **Run**.
3. Select the **Discovered Accounts** tab.  
IBM i accounts that have updates available display a green checkbox under the Updates Available column.
4. Select the **Update** button for the IBM i account with updates available.  
The Update Discovered Accounts window appears. Available Services and Scheduled Tasks appear on their respective tabs.
5. Select **OK**.
6. Select **Yes** when you are prompted to Update Selected Accounts.
7. To see a list of services and scheduled tasks:
  - a. Select **Credentials, Manage Targets, Accounts**.
  - b. Select the Services and Scheduled Tasks tabs to display the list accounts.

To remove tasks and services from an IBM i Target Accounts, follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the account that you want to modify.
3. Select **Update**.
4. Select the Services or Scheduled Tasks tab.
5. To delete a service or task, select the **X** next to the entry.

#### NOTE

**More Info:** [Use Account Discovery to Add Target Accounts](#)

## Discover Active Directory Services and Scheduled Tasks

You can use account discovery to manage credentials of multiple Windows services and scheduled tasks. To configure discovery for AD required the combination of an AD target account and a windows Proxy or Windows remote account. Using the combination that you can discover and manage updates for any services and scheduled tasks that use the AD account. You do not have to update the password on an individual service or scheduled task basis.

Discovery of services and scheduled tasks that are associated with AD accounts is based on AD domains and groups.

To configure this feature, complete the following topics:

### Complete the Prerequisites

Before you use service or scheduled task discovery, ensure that the following prerequisites are met:

- The target server and Active Directory target application are configured.
- A Windows Remote or Windows Proxy target application and administrative account is configured. You must use one of these accounts to discover the services and scheduled tasks.
- If the Windows Remote or Windows Proxy target account is of Administrator account type, the account requires Administrator rights on the Windows server.

#### NOTE

If your target account is to be used as a service account (that is, it is to be used to rotate passwords of other target accounts), we recommend that you prevent this account from being able to login interactively. To do this, assign the following User Rights to the Windows account:

- Deny log on locally
- Deny log on through Remote Desktop Service
- The administrative account to be used for discovery has been verified in Credential Manager.

### **Discover Services that Use AD Accounts**

Use service discovery to speed the process of adding services that are associated with an Active Directory target account. Discovered services are typically added to synchronized accounts so Credential Manager can manage them.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. The Target Accounts page appears.
2. Select a Target Account of the Active Directory **Application Type** to use for service discovery. The account that you select must be **Verified** (with a checkmark in the Verified column).
3. Select **Update**.
4. Ensure that the data in the fields are specified according to your requirements.
5. For Service discovery, select the **Services** tab.
6. For **Change Services Using**, select the credentials to use for changing Services:
  - **Change Process Credentials:** Use the credentials for this AD account.
  - **Proxy or Windows Remote Credentials:** Use the credentials for the Proxy or Windows Remote selected in the next step.
7. For **Discover Services**, select Windows Remote or Proxy:
  - **Using Proxy:** Select the **Proxy Host** from the drop-down list. Enter the **Host to Search** on which the services reside.
  - **Using Windows Remote Credentials:** Select the magnifying glass icon to select a target account that is an Administrator on the target server.
8. For **Login Using**, select the credentials for logging in:
  - **Change Process Credentials:** Use the credentials for this AD account.
  - **Proxy or Windows Remote Credentials:** Use the credentials for the Proxy or Windows Remote selected in the previous step.
9. Select the **Discover Services** button. The procedure returns a list of services for the account. The discovered services are added to the table on the Services tab.
10. To allow Credential Manager account to start or restart a service, select its check box in the Restart column. To disallow this feature, clear the check box.
11. Select **OK** if you want to update credentials for all the discovered services whenever the target account password changes.

#### **To add a service to the account manually, follow these steps:**

1. Select the **+** icon in the Services table.
2. In the new row, select a Proxy or Windows Remote Credential.
3. Enter the **Service Host** on which the service resides, and enter the Service name.
4. To allow Credential Manager account to start or restart a service, select its check box in the Restart column. To disallow this feature, clear the check box.
5. Select **OK** if you want to update credentials for all the listed services whenever the target account password changes.

To remove any services that are not required, select the **X** delete icon corresponding to the service in the Services table. The deleted service retains its current login credentials and is not updated when the target account password changes.

## Discover Scheduled Tasks that Use AD Accounts

Use scheduled tasks discovery to speed the process for adding the scheduled tasks that are associated with an Active Directory target account. Discovered scheduled tasks are typically added to synchronized accounts so Credential Manager can manage them.

### Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**. The Target Accounts page appears.
2. Select a Target Account of the Active Directory **Application Type** to use for Scheduled Tasks discovery. The account that you select must be **Verified** (with a checkmark in the Verified column).
3. Select **Update**.
4. Ensure that the data in the fields are specified according to your requirements.
5. For Scheduled Tasks discovery, select the **Scheduled Tasks** tab.
6. For Change **Tasks** Using, select the credentials to use for changing Scheduled Tasks:
  - **Change Process Credentials:** Use the credentials for this AD account.
  - **Proxy or Windows Remote Credentials:** Use the credentials for the Proxy or Windows Remote selected in the next step.
7. For **Discover Tasks**, select Proxy. Select the **Proxy Host** from the drop-down list. Enter the **Host to Search** on which the tasks reside.
8. For **Login Using**, select the credentials for logging in:
  - **Change Process Credentials:** Use the credentials for this AD account.
  - **Proxy or Windows Remote Credentials:** Use the credentials for the Proxy or Windows Remote selected in the previous step.
9. Select the Discover **Tasks** button. The procedure returns a list of tasks for the account. The discovered tasks are added to the table on the Scheduled Tasks tab.
10. Select **OK** if you want to update credentials for all the discovered scheduled tasks whenever the target account password changes.

### To add a scheduled task to the account manually, follow these steps:

1. Select the **+** icon in the Scheduled Tasks table.
2. In the new row, select a Windows Remote Credential.
3. Enter the **Task Host** on which the scheduled task resides, and enter the Task name.
4. Select **OK**.
5. Manually synchronize the task password with the account password.

**To remove any scheduled tasks:** In the Scheduled Tasks tables, select the **X** (delete) icon corresponding to the task. The deleted scheduled task retains its current login credentials and is not updated when the target account password changes.

### NOTE

To discover Windows Proxy services and scheduled tasks for local accounts, see [Register Windows Proxy Target Accounts](#).

To discover Windows Remote services and scheduled tasks for local accounts, see [Configure Windows Remote Target Accounts](#).

## Cisco SSH Target Account Configuration

If you configure a target account for a Cisco target application, the Cisco SSH tab is added to the Target Account page.

### NOTE

PAM supports only Cisco IOS and ASA IOS devices.

To enable the appliance to manage passwords, follow the procedure [Manage Local Accounts on Cisco IOS or ASA IOS Devices](#).

**On the Cisco SSH tab, complete the following fields:**

- **Protocol:** Select whether the connection to the target is using SSH-2 or Telnet.
- **Account Type:** Select one of the following two options. The selected option indicates which account PAM uses to change the password.
  - **Login (User EXEC):** To restrict the target account to only User EXEC permissions, select this option. Configure any other active settings on the page.
  - **TACACS+:** If the user account resides on a TACACS+ server, select this option.

#### NOTE

Do not select the **Enable (Privileged EXEC)** option. The appliance cannot manage passwords using this option.

- **Change Password for Lines:** Select which type of line on the Cisco router for which this user account can change passwords. The choices are:
  - VTY (virtual terminal) lines
  - AUX (auxiliary) port
  - Console (CTY) line for a console terminal
- **Connect As** (Available for accounts of type Login (User EXEC) only): Specify whether to use the target account or a different account. Accept the default, **This account**, to use the target account. To specify another account, select **The following account** radio button and then enter the account name.
- **Verify Through Other Account** (Available for accounts of type Login (User EXEC) only): If you specify an account other than the target account for password management, verify the user access configuration. Select one of the following options:
  - **Verify using own credentials**
  - **Verify using other account's credentials**
- **Access Privileged EXEC As** (Available for accounts of type Login (User EXEC) only): To elevate permissions to the Privileged EXEC level, select this option and specify a fake target account that holds the Enable mode password.

### Manage Local Account Passwords on Cisco Devices

To manage passwords on a Cisco IOS or ASA IOS device, the account that connects to the Cisco device must be elevated to Privileged EXEC mode. The Enable command promotes an account to Privileged EXEC mode so a user can execute privileged tasks, such as changing passwords. PAM must initially log in to the Cisco device using an account with only User EXEC permissions. That account must then be elevated to Privileged EXEC mode.

To elevate the connection to Privileged EXEC mode, configure two accounts:

- **Enable password account.** This account stores the password for the Enable command which is used to execute Privileged EXEC level tasks. You must know the Enable password to create this account.
- **Standard User EXEC account.** This account initially logs in to the Cisco device.

The following procedures explain how to configure these two accounts.

#### **Configure the Enable Password Account**

Set up an account that holds the Enable command password. This account is a fake account that does not exist at the Cisco device. After you create this account, you can use it for any standard user account that you want to promote to Privileged EXEC level.

**Follow these steps:**

1. Create a target account that is associated with the Cisco target application.
2. On the Account tab:

- For the Account Name field, assign a name that indicates the purpose of this account, such as enableacct.
- In the Password field, enter the Enable password.

### Update enableacct

Account
Password
Compound Servers
Cisco SSH

Host Name: *	<input type="text" value="111.11.1.12"/>	<input type="text" value="Password: *"/>
Device Name: *	<input type="text" value="Cisco"/>	<input type="checkbox"/> Show Password:
Application Name: *	<input type="text" value="ciscoswitch"/>	
Account Name: *	<input type="text" value="enableacct"/>	
Password View Policy: *	<input type="text" value="Default"/>	
Account Type:	<input type="text" value="Privileged Account"/>	
Access Type:	<input type="text"/>	
Descriptor 1:	<input type="text"/>	
Descriptor 2:	<input type="text"/>	

- On the Password tab, ensure that the Synchronized setting is using the **Update only the Credential Manager Server** option.
- On the Cisco SSH tab, use the following settings:
  - Account type: Login (User EXEC)
  - Connect As: This account
  - Access Privileged EXEC As: This account



## Update enableacct

Account Password Compound Servers **Cisco SSH**

Protocol:
☒ SSH-2 Password or Keyboard-Interactive Authentication
☐ Telnet

Account Type:
☒ Login (User EXEC)
☐ Enable (Privileged EXEC)
☐ TACACS+

Change Password for Lines:
☐ VTY  Maximum VTY Number
☐ AUX
☐ Console

Connect As:
☒ This account
☐ The following account

Access Privileged EXEC As:
☒ This account
☐ The following account

5. Select OK.

### Configure Standard User Account

After creating the Enable password account, create an account with User EXEC permissions. This account uses the Enable account to elevate its permissions. This user can then update passwords.

#### Follow these steps:

1. In the UI, create a Cisco target account that is associated with the Cisco target application. For this example, the account name is ciscouser.
  2. On the Account tab, enter the current password for the account at the Cisco device.
  3. On the Password tab, change the Synchronized setting to **Update both the Credential Manager Server and the target system.**
  4. On the Cisco SSH tab, use the following settings:
    - **Account type:** Login (User EXEC)
    - **Connect As:** This account
    - **Access Privileged EXEC As: The following account:** Select the Enable account. In this example, that account is enableacct.
  5. Select **OK** to save the account
- The following picture shows an example:

## Update ciscouser

Account	Password	Compound Servers	Cisco SSH
Protocol:	<input checked="" type="radio"/> SSH-2 Password or Keyboard-Interactive Authentication <input type="radio"/> Telnet		
Account Type:	<input checked="" type="radio"/> Login (User EXEC) <input type="radio"/> Enable (Privileged EXEC) <input type="radio"/> TACACS+		
Change Password for Lines:	<input type="checkbox"/> VTY <input type="text" value="1"/> Maximum VTY Number <input type="checkbox"/> AUX <input type="checkbox"/> Console		
Connect As:	<input checked="" type="radio"/> This account <input type="radio"/> The following account		
Access Privileged EXEC As:	<input type="radio"/> This account <input checked="" type="radio"/> The following account		
<input type="text" value="enableacct"/>			

PAM can now use this standard user account (ciscouser) to manage passwords for other Cisco accounts, both standard and privileged.

If you configure more accounts, you can use this standard user account to manage passwords. For those other accounts:

- For the **Connect As** option, select **This following account** and specify the standard user account.
- Leave the **AccessPrivileged EXEC As** option set to **This account**

## SSH Key Authentication for Accessing UNIX/LINUX Targets

For SSH access to a UNIX/Linux target server, you can use SSH key pairs instead of a password to authenticate a client to an SSH server.

To configure SSH key authentication, you must:

1. Create an SSH key pair policy using the UI or generate a key pair using a third-party utility. If you use a utility, copy the key pair to a local system from which you can upload them into the credential database.
2. Create a UNIX target application and select the SSH Key pair policy that you created.
3. Configure a target account that is associated with the UNIX target application. For the account, set the Protocol field to SSH-2 Public Key Authentication.
4. Create an access policy that uses the SSH key pair.

Complete the following procedures:

## **Create an SSH Key Pair Policy with the UI**

For the appliance to generate an SSH key pair, configure an SSH key policy. The key policy specifies the characteristics for the key pair, specifically the cryptographic algorithm, and the key size. When you update the target account that uses the key pair, the appliance pushes the public key to the target device.

### **Follow these steps:**

1. Select **Credentials, Manage Targets, SSH Key Pair Policies**.
2. Select **Add**.
3. Provide a unique **Name** for the policy.
4. (Optional) Provide a **Description** for the policy.
5. Select the **Key Type**: ECDSA or RSA or DSA.
6. Specify the **Key Length**. The drop-down list shows the options available for the key type.
7. Select **OK**.

After you create a key pair, you can select it when you configure a target application.

## **Select the SSH Key Policy for the UNIX Target Application**

Remember to configure a UNIX/LINUX target device before you create a target application.

### **Follow these steps:**

1. Select **Credentials, Manage Targets, Applications**
2. Select **Add**.
3. In the Add Target Application dialog, complete the fields, selecting **UNIX** for the **Application Type**. Several more tabs populate the page.
4. Select the **SSH-2** tab.
5. In the **SSH Key Pair Policy** field, select the key pair policy.
6. Select **OK**.

## **Add the SSH Key Pair to a Target Account**

### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add**.
3. Complete the fields, noting the following specific entries:
  - **Application Name**: Search and select the UNIX target application that you created.
  - **Account Name**: Enter a valid account name on the target device
  - **Protocol**: Select SSH-2 Public Key Authentication
4. Do *one* of the following tasks:
  - For the appliance to generate the key pair, select the keys icon next to the Private key box.
  - To upload keys that are generated by a utility, select **Choose File** next to the Private and Public key boxes. Browse to the relevant file on your local system.
5. Select the **Password** tab and for the **Synchronized** setting, select **Update both the Password Authority Server and the target system**.
6. Select **OK**.  
In the list of target accounts, a green checkmark in the Verified column next to the specific account indicates that the keys were verified.

## **Create an Access Policy that Uses the SSH Keys**

After you configure your target components, can now manage access to the target server by creating a policy.

### **Follow these steps:**

1. Select Policy, Manage Policies.
2. Select Add.
3. On the Association tab, select the user.
4. on the Access tab, select **SSH:22**.
5. For that access method, search for the target account you created earlier.
6. Select **OK**.

## **Test SSH Access using SSH Key Authentication**

The appliance can now authenticate to the UNIX target using the SSH key pair. The target server uses the public key to authenticate. When the appliance connects to the target using SSH, it uses the private key. The target server authenticates the access request using the public key.

### **Follow these steps:**

1. As the user, log in to the UI and select the Access page.
2. Select the SSH icon for the target server to launch an SSH session.
3. When the command window opens, view the public key by entering:

```
cat .ssh/authorized_keys
```

## **Securing Privileged Accounts that use SSH Keys**

Privileged Access Manager secures privileged accounts by preventing users from knowing the account passwords. When you initially deploy the appliance in your environment, you configure the appliance to change the passwords for those accounts. If SSH keys for those privileged accounts exist before you deploy the appliance, changing the passwords does not prevent the existing SSH keys from working. So, those privileged accounts are not fully secure.

SSH key discovery allows you to seek out these keys so you can remove them. Once removed, the privileged accounts are truly secured; you can only use them through the appliance. Learn how to use SSH key discovery by reading [Use SSH Key Discovery to Find Key Pairs](#).

## **Use SSH Key Discovery to Find Key Pairs**

An administrator can install SSH keys to protect access to privileged accounts. When you initially deploy the appliance in your network, you configure the appliance to change your privileged account passwords. However, if you deploy the appliance *after* SSH keys are installed, changing the passwords does not stop the SSH keys from working. So, those privileged accounts are not fully secure.

SSH key discovery allows you to find these keys so you can remove them. Once removed, the privileged accounts are truly secure, and only the Privileged Access Manager can manage these privileged accounts. SSH key discovery does not manage private keys of privileged users.

### **NOTE**

SSH key discovery only occurs for application types Linux and UNIX.

The following topics explain how to run SSH key discovery:

## Prerequisites

Before you perform SSH key discovery, complete the following prerequisites:

- Enable Account Discovery at the target application and target account
- Grant sudo permissions to the administrative account
- Edit the sudoers file to disable password authentication

### **Enable Account Discovery at the Target Application and Target Account**

SSH key discovery requires that you set up account discovery. For configuration instructions, see [Account Discovery](#).

1. Select a target application type that supports account discovery, such as UNIX.
2. Optionally, configure the options on the **Account Discovery** tab. This tab does not enable account discovery but it defines other options. Account Discovery is enabled at the target account, by selecting the Discovery Allows checkbox. The options on the tab differ depending on the application type. For example, a UNIX application provides the UID and GID values or ranges, which limit the number of discovered accounts. The UID and GID settings are used in conjunction, so that the targets must satisfy *both* criteria to be discovered.
3. Configure a target account to allow discovery. Add a target account, select the Password tab, and select the **Discovery Allowed** checkbox.

The appliance uses only those accounts with Discovery Allowed enabled as credentials for discovery.

If **Discovery Allowed** is checked, the "Allow multiple server discovery for this type of application" checkbox is also displayed for UNIX accounts. This checkbox lets the account act as a global discovery account for any server and application of this type. For example, if you have 20 servers with a common account and password, use one account and select this box. Then for any discovery job with this application type selected, this account is used as a credential for discovery.

### **Grant sudo Permissions to the Administrative Account**

Grant sudo permissions to the administrative account doing the discovery on the remote target system. SSH key discovery skips any accounts with inadequate permissions.

An administrator can create SSH keys for specific privileged accounts. For SSH key discovery, the administrative account uses sudo with the following commands:

- test
- cat
- date
- ssh-keygen

To test whether an account has sufficient access, issue one of these commands while logged on using that account. For example:

```
sudo -l ssh-keygen
```

Successful commands echo the full command name, while failures report insufficient access:

```
Sorry, user user may not run sudo on [server].
```

### **Edit the sudoers File to Disable Password Authentication**

If the administrative account uses only SSH key pairs instead of a password, configure the target server not to ask for a password.

To prevent the administrator from being prompted for a password, edit the **sudoers** file by adding a NOPASSWD entry for the account. For example:

```
jdoe ALL=(ALL) NOPASSWD: ALL
```

#### Follow these steps:

1. On the remote target server, edit the sudoers file in the */etc* directory.
2. Find the entry for the administrative account.
3. Add NOPASSWD to its entry. For example:

```
jdoe ALL=(ALL) NOPASSWD: ALL
```

4. Repeat for each server that is targeted for SSH key discovery.

### Process to Discover Keys

To perform discovery of SSH keys, follow these steps:

1. Create a scan profile.
2. Run the scan and view results.
3. View the scan results in the scan profile history.
4. (Optional) Export the results to a CSV file.

### Add and Run a Scan Profile

Start by adding a Scan Profile. Follow these steps:

1. Select **Credentials, Discovery**.
2. Select the **Scan Profiles** tab and select the **ADD** button.  
On the **Profile** tab, name the profile, and give it an optional description. Purge Interval sets the number of days after which devices that are discovered by this scan are deleted. Devices that have also been discovered by another profile are not deleted. The Purge Interval default is set on the Global Settings page, under Basic Settings, as Scan Purge Interval.
3. On the **Servers** tab, move **Available Servers** to the **Selected Servers** column. The Available Servers list is populated by managed devices.
4. Optionally, create a schedule to run the scan. Otherwise, skip to the next step to run the scan on demand.
  - Select the **Schedule** tab.
  - Select a **Frequency**. Other fields appear.
  - Select the appropriate time intervals.
  - Select **OK** to save the scan profile.
5. Select **OK** to save the scan profile and return to the Device Scan Profiles list. Select the scan profile from the list and select **RUN**.

#### NOTE

Selecting **Delete** for a highlighted Scan Profile deletes its scan profile history. It also deletes any accounts that are associated with that profile, unless they are associated with another profile.

### **Monitor the Scan**

You can monitor the progress of a scan on the **Scan Profile Jobs** tab. You can also cancel the job on this panel by selecting **CANCEL JOB**. Once a job is complete, view a summary of its results on the Scan Profile History tab.

Tables in the Discovery area allow filtering by column values. You can use asterisks and percent signs as multiple-character wildcards.

### NOTE

The Scan Profile Jobs and other tables are refreshed according to the value of the **Table Refresh Interval** field. This field is on the first tab of the Global Settings page. The default refresh time is 60 seconds.

### View the Scan Results

Select the **Scan Profile History** tab to view the results of the discovery scans. Each row shows a Scan Profile, its latest Discovery time. You can also select the buttons to view different aspects of a scan. The Summary also displays the number of errors encountered. These numbers refer only to the latest run of this scan profile.

For account discovery scans, see [Account Discovery](#).

### View Summary Details Display

The View Summary Details button opens the scan results window. The summary shows the following information:

- A count of discovered keys, how many are new, and not found. "Not found" keys were discovered by a previous run of the same scan profile, but are now missing.
- Scan Information tab displays the scan profile name and the job time.
- The Discovered Keys, New Keys, and Not Found Keys tabs list the Account Names and SSH key fingerprints in each respective category.

The Logs tab displays a table including each action that is taken regarding this scan.

### View Key Scan Results

To view key scan results, select a profile on the Scan Profile History page then select the **View Key Scan Results** button. The following information about the discovered keys is available:

Field	Description
Account Name	One or more accounts that are associated with an SSH key. If you export the results to a CSV file, this field is named userIds.
Fingerprint	Shows the public key fingerprint as hex pairs separated by colons.
Key File Age	The number of days when the key file was last modified. This number of days might not be the age of the key itself.
Key Size	The size (or length) of the SSH key in bits
Device Name	The server where the key was discovered. If you export the results to a CSV file, this field is the targetServerName.
Authorized Key File Name	The location of the <code>authorized_keys</code> file. The names of the SSH keys are stored in this file.
Is Managed (read only)	If the appliance manages the SSH key, this checkbox is selected. To enable the appliance to manage a key, the existing keys at the remote target must first be revoked manually. Then, generate a new key pair with the appliance. Only SSH keys that are generated and deployed with Credential Manager are managed.

The **Export** button creates a CSV file with a row for each discovered account that is listed.

The **View** button opens the View Discovered Keys dialog for the Account Name whose box is checked. The dialog has a **Basic Info** and **Advanced Info** tab. The Advanced Info tab displays log information that is not shown in the Account Scan results panel.

## Discovered Keys

The Discovered Keys tab contains the same information as the [View Key Scan Results](#). From this tab, you can select accounts and view details about discovered keys.

### View Discovered Keys

To open the View Discovered Key page for an account, select the account entry on the Discovered Keys page then select **View**. The **Basic Info** tab of the page contains the same information as the Discovered Keys tab.

The **Advanced Info** tab provides the following additional information:

Field	Description
Key	Displays the entire public key, including the modulus or base64 key. For SSH protocol 1, only RSA is supported (rsa1). For SSH-2, base64 is displayed.
Key Instance	It is possible to duplicate the <code>authorized_keys</code> text file so this field maintains data consistency. Any duplicate keys have an incremented integer here, typically 1.
Key Type	Displays the type of SSH key.
Comment	SSH key generation allows inclusion of comments in the key file, which are displayed in this field if present.
Revoked	Some systems are configured to allow an SSH key to be revoked. Key discovery tests each key to see if it was revoked using the command <code>"ssh-keygen -Q"</code> . If so, that is saved as a property.
Bubble Babble	Bubble Babble is an encoding method for binary data fingerprints. The bubble babble format renders the hexadecimal digits into pseudowords that can be pronounced more easily than a series of hexadecimal digits.

### Export Discovered Keys to a File

You can export information about discovered SSH keys to a CSV file for use in spreadsheets and databases. To export all SSH keys, select the Discovered Keys tab. Select the Export button above the displayed list to generate a CSV file. To export data from a specific scan, select the Scan Profile History tab. Select a Scan Profile, then select View Key Scan Results. The Export button appears above the list of keys.

The exported CSV file contains more information than is displayed in the UI. In addition to what is found in the UI, the following fields are included:

- **targetApplicationName:** The name of the target application
- **protocolVersion:** SSH Protocol 1 or 2
- **options:** Login options as included in the SSH key file
- **exponent:** Part of SSH protocol 1 (RSA1) key, with values such as 65527
- **modulus:** Part of SSH protocol 1 (RSA1) key, a long integer
- **base64Key:** Part of SSH protocol 2 key, a long base64 representation of the public key
- **authorizedKeyFileTimestamp:** The timestamp of the authorized key file, used to determine Key File Age field
- **lastLogin:** Displays the last time that this key was used to log in, as determined by its last log entry. If the log file does not go far back enough, this field might be blank



## SSH Certificate Authentication for Accessing UNIX/LINUX Targets

When connecting to target devices using SSH protocol, PAM can be configured to use Certificate Authentication as an alternative to password or public key authentication. SSH Certificate Authentication establishes a chain of trust through the PAM SSH User Certificate Authority. This certificate-based approach requires a public key for the certificate authority to be added to the target system **TrustedUserCAKeys** file.

Certificate authentication reduces the administrative burden of maintaining authorized keys or passwords on target devices therefore providing zero standing privileges for the Target systems. Also, certificates that are issued by PAM can specify a validity period providing Just-In-Time access. Combine this with the ability to control authorized activities by specifying options for the certificate user and SSH Certificates provide an excellent contribution to an organization's Zero Trust strategy.

To configure SSH certificate authentication, complete the following procedures:

### 1. Configure PAM as an SSH Certificate Authority

As a Configuration, Super, or Global administrator, you can use PAM as an SSH certificate authority (CA) to provide your organization members with the ability to authenticate using signed SSH certificates.

#### NOTE

**Prerequisite:** PAM's SSH Certificate Authentication capability depends on SSH Certificates that are generated at login time and have a brief validity interval. As a result, your PAM instances and your Unix Target Devices **must** have their system clocks synchronized. We recommend, but do not require use of NTP on your PAM instances and your UNIX Target Devices so that their system clocks are always synchronized. For more information about clock synchronization, see [Configure Date/Time Settings](#).

#### Follow these steps:

1. Select **Configuration, Security, SSH Certificate Authority** to display the **SSH Certificate Authority** page. The first time this page appears, it displays only one button that is labeled **Enable SSH Certificate Authority**.
2. Select the **SSH Certificate Authority** button to enable PAM to function as an SSH Certificate Authority. Configure the following options as desired.
3. In the **Algorithm** drop-down, select either **ECDSA** or **RSA**. This choice determines corresponding the **Key Size** options: **ECDSA** supports 256 and 384, and 521. **RSA** supports 2048 and 4096.
4. In the **Key Size** drop-down, select the key size.
5. Select **Save and Generate**. The **Public Key** textbox displays the generated public key. You can copy the public key to the UNIX and Linux target devices, as shown in the following section.

### 2. Copy the Public Key from the Certificate Authority to the Target UNIX/Linux Systems

As root user, you must copy the public key from created in the Certificate Authority page in the previous step to the **TrustedUserCAKeys** file on the target device to establish trust. You have two options when using deciding how to distribute the public key:

- [Use the Manual Method to Distribute the Key](#)
- [Use a Scripted Method to Distribute the Key](#)

#### Use the Manual Method to Distribute the Key

Use these manual steps to distribute the public key. For more information about OpenSSH Server configuration, see [https://man.openbsd.org/sshd\\_config](https://man.openbsd.org/sshd_config).

#### Follow these steps:

1. On the target device, modify the sshd configuration file `/etc/ssh/sshd_config` to set the **TrustedUserCAKeys** parameter to a local file (`/etc/ssh/ca.pub` for example).

2. As the root user, copy the public key from the PAM SSH Certificate Authority created in the previous section to the `/etc/ssh/ca.pub` local file.
3. Restart `sshd` on the target device by entering the following command: `$ /bin/systemctl restart sshd.service`
4. Repeat these steps for every target UNIX/Linux device.

### ***Use a Scripted Method to Distribute the Key***

As an administrator, you can also use a script to retrieve the current SSH Certificate public key from the specified PAM instance, and apply it to the local SSHD service. The script downloads the public key from the PAM SSH Certificate Authority using a public, unauthenticated REST API call. Comments within the script itself give well-documented instructions on how to use it.

#### **NOTE**

You must copy the script and must run it on each UNIX machine.

#### **Follow these steps to use a script to distribute public key:**

1. To access the script, select [this link](#) to download a zip file that contains the script.
2. Unzip the file to access the script.
3. Follow the comments in the script for more instructional information.

### **3. Create an SSH Certificate Policy**

As a System Administrator for UNIX and Linux devices, you can configure SSH Certificate Authentication options and extensions to further control the use of managed devices. The options and extensions themselves are described in the OpenSSH Certificate man page, which is defined [here](#). A subset of the defined options and extensions can be configured using the SSH-Certificate Policy UI which can then be attached to a UNIX target application.

#### **NOTE**

There is a default SSH Certificate Policy named "Default". If you had an existing policy named "Default" before upgrading, that policy becomes the default. Also note that you cannot delete the default policy, but you can modify it.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, SSH Certificate Policies**.
2. Select **Add** to display the **Add SSH Certificate Policy** window.
3. Provide a unique **Name** for the policy.
4. (Optional) Provide a **Description** for the policy.
5. (Optional) In the **Force Command** field, enter a force command string. This value forces the execution of the command that is entered in this field instead of opening a shell.
6. Select the desired **Extensions**. You can select the following optional extensions, and then select **OK** to confirm and exit this window:
  - **X11 Forwarding**: X11 forwarding is a mechanism that allows a user to start up remote applications and forward the application display to your local system display.
  - **Port Forwarding**: SSH port forwarding creates a secure connection between a local computer and a remote machine through which services can be relayed.
  - **Pseudo Terminal**: This setting allows Pseudo Terminal (aka PTY) to be allocated.
  - **User Run Commands**: Allows execution of the user `~/.ssh/rc` file at login time.

### **4. Create a UNIX Device**

Create a device, as described in [Device Setup](#), with these options:

- On the **Basic Info** tab: Select **Password Management**, and set the Name and **Address** for a UNIX device.
- On the **Access Method** tab, select **SSH** if you want PAM to use MindTerm. Select **X11** if you want to use X11.
- You can also [Create an SSH Service to Access a Device](#) with the **Protocol** set to **TCP**, the **Application Protocol** as **SSH**, and set the **Client Application** to (for example, for PuTTY)

```
C:\Progra~1\PuTTY\PuTTY.exe -ssh -l <User> <Local IP> <First Port>
```

#### NOTE

If you want to use X11 Forwarding, you must set the **X11** option and you must modify your PuTTY Client Application command to include the “-X” switch.

- If you do use a service, make sure to add the service to the device. For more information, see the [Select Services](#) section of the [Device Setup](#) topic.

### 5. Add a UNIX Target Connector

Use the UNIX target connector to manage UNIX-based privileged accounts.

Create a UNIX Target Connector, as described in [Add a UNIX Target Connector](#), with these options:

- On the **Application** tab, in the **Application Type** field, select **UNIX**.
- Select the **Host Name** corresponding to the Device that you created earlier.
- On the **SSH-2** tab, select the desired **Key Pair Policy** and **Certificate Policy**. For information about key pair policies, see [SSH Key Authentication for Accessing UNIX/LINUX Targets](#).

#### NOTE

DSA key types are incompatible with SSH-2 Certificate Authentication.

### 6. Add the SSH Certificate Target Account and Add Target Accounts to Target Applications

After you configure a Unix Target Connector, you can add corresponding target accounts. Target accounts identify accounts at the remote server for which PAM can authenticate users using SSH-2 certificate authentication. This section follows the [Add Target Accounts to Target Applications](#) topic with the same exceptions for SSH-2 certificate authentication configuration items.

#### Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add**. On the **Account** tab, complete the fields, noting the following specific entries:
3. In the **Application Name** field, search for and select the UNIX target application that you created.
4. In the **Account Name** field, enter a valid account name for the target device.
5. In the **Protocol** field, select **SSH-2 Certificate Authentication**. This option displays the following fields:
  - a. **Principal**: Optionally, enter a comma-separated list of strings to use as authentication principals. If this field is blank, the **Account Name** is used as the principal. The principals that are defined here should match the principals that are defined on the SSH server.
  - b. **Certificate Details**: Lists the details of the selected SSH certificate authentication policy that is associated with the target application.
6. The **Certificates** tab appears when you select **SSH-2 Certificate Authentication** for your **Protocol**. This tab displays the following options:
  - a. **Last Generated**: Displays the most-recent time and date that the certificate was generated. A new certificate is generated and sent to the SSHD server on the UNIX system every time a user logs in using MindTerm or an SSH proxy service. **Last Generated** is equivalent to the last time that a user attempted to log in with this target account.
  - b. **Account Created**: Displays the time and date that the account was created.
7. Select **OK** to confirm and exit this page, and add the new target account to the list of accounts on the **Account List** page.

## 7. Create an Access Policy that Uses the SSH Certificate

After you configure your target components, can now manage access to the target server by creating a policy.

**Follow these steps:**

1. Select **Policy, Manage Policies**.
2. Select **Add**.
3. Complete the fields, noting the following specific entries:
4. On the **Association** tab, select the **User** and **Device**.
5. On the **Access** tab, select the SSH Access Method if one was configured in the **Device**.
6. For the **Selected Access** method, search for and add the target account that you created earlier.
7. Select **OK**.

### Special Considerations For SSH Access Method Sessions Using SSH-2 Certificate Authentication

When using the SSH-2 Certificate Authentication protocol, the SSH Access Method autologin behavior differs from autologin using the SSH-2 Password or SSH-2 Public Key protocols. When using SSH-2 Certificate Authentication, the applet connects to an SSH Proxy Service in the PAM appliance that performs go-between actions including SSH-2 certificate authentication, session recording, command filtering and socket filtering. The SSH-2 Password or SSH-2 Public Key protocols do not require this additional layer of processing.

As a result, using the SSH-2 Certificate Authentication protocol reduces the number of simultaneous SSH Access Method applets per PAM Appliance that can be run due to increased load on the PAM server. Also, the cryptography settings governing connections to Target Devices via the SSH-2 Certificate Authentication protocol will be configured on the **Configuration, Security, Cryptography** page under the **SSH Proxy** tab, versus the **SSH MindTerm** tab for the SSH-2 Password or SSH-2 Public Key protocols.

### Troubleshooting

#### Using X11 with Certificates

If you want to use X11, be sure to select it in the certificate, during device setup, and to select X11 and enter the correct syntax for X11 in the **Client Application** text box.

## Create an SSH Certificate Policy with the UI

As a System Administrator for multiple UNIX and Linux devices, you configure Certificate Authentication options and SSH certificate extensions to control the permitted activities, commands, and validity period of Users connecting to managed devices. This configuration improves the ability to define roles and limit User activities to that authorized. Such options are shown in the openSSH Certificate man page, defined [HERE](#), and are available to establish a SSH-Certificate policy to apply to accounts used to connect to target systems by users.

### NOTE

There is a default policy named Default. If you have an existing policy named default, that policy becomes the default. Also note that you cannot delete a policy named default.

**Follow these steps:**

1. Select **Credentials, Manage Targets, SSH Certificate Policies**.
2. Select **Add** to display the **Add SSH Certificate Policy** window.
3. Provide a unique **Name** for the policy.
4. (Optional) Provide a **Description** for the policy.

5. (Optional) In the **Force Command** field, enter a force command string. A force command forces (or overrides) the execution of the command entered in this field instead of any shell or command specified by the user when using the certificate for authentication.
6. Select the desired **Extensions**. You can select the following optional extensions:
  - **X11 Forwarding**: X11 forwarding is a mechanism that allows a user to start up remote applications but forward the application display to your local system display.
  - **Port Forwarding**: SSH port creates a secure connection between a local computer and a remote machine through which services can be relayed. When you use port forwarding, the client still thinks that it connects to the hostname/IP address of the gateway. When the SSL certificate is used to verify the host name, as you do with https, the SSL certificate you serve from the server should be valid for the host name of the forwarding gateway.
  - **Pseudo Terminal**: A Pseudo Terminal (aka pseudoterminal) is a pair of virtual character devices that provide a bidirectional communication channel.
  - **User Run Commands**: Allows execution of `~/.ssh/rc`
7. Select **OK** to conform and exit this window.

After you create an SSH Certificate Policy, you can select it when you configure UNIX and Linux target application.

## Set the Privilege Elevation for UNIX Target Accounts

For target accounts associated with UNIX target applications, you can configure the **Privilege Elevation** setting. This setting determines which privilege elevation capabilities the account has on the target server. How you configure this setting impacts whether password synchronization works.

On the UNIX tab of the target account, select one of the following options for the given account.

### NOTE

The descriptions assume that the privilege elevation command is **sudo** and the password change command is **passwd**.

- **Do not use elevated privileges**: Select this option for an account that is not allowed to run sudo commands on the target server. When the user of the account tries to change its own password, the user must provide the current password first. Accounts without privilege elevation cannot update passwords of other accounts.
- **Use elevated privileges**: Select this option for an account that is allowed to run sudo commands without providing its own password to sudo. This use case applies for an account with the "NOPASSWD" flag set in the `/etc/sudoers` file. The NOPASSWD flag is considered insecure and not recommended. Such accounts can change passwords of other accounts, including the root account.
- **Use elevated privileges with authentication**: Select this option for accounts that can run sudo commands but must provide a password. Before a command is executed, the sudo command prompts the account user for a password. This behavior is the recommended sudo option. Such accounts can change passwords of other accounts, including root.
- **This account is a root account**: Select this option for accounts that need no privilege elevation. Such accounts can change their own password without having to provide the current password first. These accounts also can change passwords of other accounts without the use of the sudo command. Beginning with release 3.0.3, if you select this option, the default script does not invoke the sudo command.

## Oracle Target Account Configuration

The Oracle target connector can communicate with an Oracle database and Oracle Internet Directory (OID) server.

If you create a target account for an Oracle target application, there are more settings that you must configure, as shown in the following screen:

## Add Target Account ? X

Account Password Compound Servers **Oracle**

Use OID:

☒ JDBC Thin  
☐ JDBC Thin using OID

Schema: \*

Schema is a RAC Service Name:

☐

Change Process:

☒ Account can change own password  
☐ Use the following account to change password

This is a SYSDBA Account:

☐

Use REPLACE Syntax:

☐

The configuration settings include:

**Use OID**—Specifies whether PAM connects to an Oracle database or an Oracle Internet Directory (OID) server. The options are:

- **JDBC Thin**: To connect to an Oracle database, accept this default option
- **JDBC Thin using OID**: To connect to an Oracle Internet Directory server, select this option and enter values for the following fields:
  - **SID/Service** – Specifies the System Identifier (SID) of the Oracle Internet Directory database instance. Enter the SID specified during the installation of the OID software.
  - **CN** – Specifies the Common Name (CN) of an Oracle context. The default value is cn=OracleContext.

**Schema**: Enter the schema name for the database account.

**Schema is a RAC Service Name** (for JDBC Thin only): If the target is an Oracle RAC, select this checkbox.

**Change Process**: Select one of the options:

- **Account can change own password**: Select this option when a user account can change the password. The assumption is that the user knows the original password.
- **Use the following account to change password**: Select this option to use a *master account*. A master account has privileges to change any account password, such as an administrator with maximum privileges.

For more information about this setting, see [Use an Alternate Account to Change Passwords \(Optional\)](#).

**This is a SYSDBA Account**: If the target account is a SYSDBA database administrator, select this checkbox.

**Use REPLACE Syntax**: The Oracle REPLACE function lets you replace one text string with another. By default, this option is not enabled. Accept the default if the account that is specified to change an account password does not know the original password.

Follow these guidelines:

- For a standard user who knows the original account password, select this checkbox. For this account, the **Account can change own password** option is also selected.
- For an account with the ALTER USER privilege, such as an Oracle administrator, acting as a master account, keep this checkbox unselected. A master account can change any account password without knowing the original password for the target account. To use a master account, select the **Use the following account to change password** setting and enter the privileged account.



## Palo Alto Account Configuration

If you configure a target account for a Palo Alto target application, the Palo Alto tab is added to the Target Account page. Select the type of account that PAM uses to manage passwords on a Palo Alto device:

**Account type:** This setting indicates whether the account is a standard user account or an administrator account.

- **User (Configuration access is disabled)** - The account is a standard user account.
- **Privileged (Configuration access is enabled)** - The user is a privileged administrator with permissions to manage other account passwords

**Connect As:** If you select User for the Account type field, select one of the following options:

- To use the specified target account, accept the default, **This account**.
- To enter an account other than the target account, select **The following account** and enter the account name.

If you change the account type from User to Privileged, the information for the Connect As setting is removed because it is no longer relevant.

## Configure Windows SSH Key Target Accounts

Learn how to configure target accounts for PAM Windows SSH Key target applications.

This topic describes how to configure Windows SSH Key target accounts.

**Follow these steps:**

1. Select **Add**.
2. Select **Credentials, Manage Targets, Accounts**. The **Target Accounts** page opens with a list of existing accounts.
3. Select **Add**. The **Add Target Account** page appears.
4. Select the **Host Name** magnifying glass icon and select the required target server from the Target Servers dialog that opens. The **Host Name** and **Device Name** fields are populated appropriately.
5. Select the **Application Name** magnifying glass icon and select the required Windows SSH Key or Windows SSH Password target application from the **Target Applications** dialog that opens. The **Application Name** field is populated appropriately.
6. Complete the following fields:
  - **Account Name:** Enter a valid account name on the target device.
  - **Password View Policy:** The default password view policy is always assigned. Use the magnifying glass icon to select other defined view policies.
7. Use *one* of the following methods to populate the public and private keys:
  - To have PAM generate the key pair, select the key icon next to the **Private Key** box. The **Public Key** and **Private Key** fields are populated using the generated values.

### TIP

To configure PAM to generate the key pair when creating a target account, select the **Use a different account to change credentials** option on the **SSH** tab.

- To upload keys that you have generated using a utility, select the Upload icons beside the **Public Key** and **Private Key** fields and select the required files to upload. The corresponding fields are populated using the uploaded keys.
8. Optionally, on the **Password** tab, change the **Synchronized** value to specify a different password synchronization option:
    - **Update only the Credential Manager Server:** Passwords are updated only in Credential Manager. Credential Manager and target system passwords can differ.
    - **Update both the Credential Manager Server and the target system** (Default): Password updates are performed in Credential Manager and on the target system to maintain consistency.

9. Select the **SSH** tab and specify the account that has the authority to change passwords using one of the following **Change Process** options:
  - **Account can change own credentials:** (Default) Allow the target account to change its own password. The initial password that you enter must be the same as the target account password.
  - **Use a different account to change credentials:** Select the magnifying glass icon next to the **Account to change credentials with** field and select the account to use to change passwords from the **Target Accounts** dialog that opens. Select an account of application type "Windows SSH Password" or "Windows SSH Key." Do not select the current target account.

**NOTE**

In the list of target accounts, a green checkmark in the Verified column next to the specific account indicates that its keys are verified.

10. Select **OK**.

**NOTE**

For information about the associated target application, see [Add a Windows SSH Key Target Connector](#).

## Configure Windows SSH Password Target Accounts

Learn how to configure target accounts for PAM Windows SSH Password target applications.

This topic describes how to configure Windows SSH Password target accounts.

### Follow these steps:

1. Select **Add**.
2. Select **Credentials, Manage Targets, Accounts**. The **Target Accounts** page opens with a list of existing accounts.
3. Select **Add**. The **Add Target Account** page appears.
4. Select the **Host Name** magnifying glass icon and select the required target server from the Target Servers dialog that opens. The **Host Name** and **Device Name** fields are populated appropriately.
5. Select the **Application Name** magnifying glass icon and select the required Windows SSH Password target application from the **Target Applications** dialog that opens. The **Application Name** field is populated appropriately.
6. Complete the following fields:
  - **Account Name:** Enter a valid account name on the target device.
  - **Password View Policy:** The default password view policy is always assigned. Use the magnifying glass icon to select other defined view policies.
7. Specify the SSH password in the **Credential** field.
8. Select the **SSH** tab and specify the account that has the authority to change passwords using one of the following **Change Process** options:
  - **Account can change own credentials:** (Default) Allow the target account to change its own password. The initial password that you enter must be the same as the target account password.
  - **Use a different account to change credentials:** Select the magnifying glass icon next to the **Account to change credentials with** field and select the account to use to change passwords from the **Target Accounts** dialog that opens. Select an account of application type "Windows SSH Password" or "Windows SSH Key." Do not select the current target account.

**NOTE**

In the list of target accounts, a green checkmark in the Verified column next to the specific account indicates that its keys are verified.

9. Optionally, on the **Password** tab, change the **Synchronized** value to specify a different password synchronization option:



- **Update only the Credential Manager Server:** Passwords are updated only in Credential Manager. Credential Manager and target system passwords can differ.
- **Update both the Credential Manager Server and the target system (Default):** Password updates are performed in Credential Manager and on the target system to maintain consistency.

10. Select **OK**.

#### NOTE

For information about the associated target application, see [Add a Windows SSH Password Target Connector](#).

## Set Up Password Composition and View Policies

Privileged Access Manager is the master password `pwd` repository that pushes password changes to the configured target accounts. You can manage privileged account passwords with the following types of password policies:

- **Password composition policies:** These policies define the rules to which passwords must conform. When passwords are updated at the target, they must comply with the composition policies.
- **Password view policies:** These policies specify how the [appliance](#) behaves when someone wants to view a password. Password view policies can also control the actions that take place after a password is viewed.

In addition to privileged accounts, you can also [manage A2A passwords](#), provided you have the correct license.

**Table 1: Test**

Policy	Definition	Use Case
Password Composition	© self-evident #	Govern password content
Password View	© self-evident #	Govern password usage

To set up password policies, see the following topics:

- [Construct Password Composition Policies](#)
- [Establish Password View Policies](#)

## Construct Password Composition Policies

Password composition policies define the rules to which target account passwords must conform. Credential Manager allows you to define various password composition policies to ensure that passwords meet the unique security needs of your organization.

If no policy is set, the default password composition policy is applied. The default policy specifies a minimum length of four characters and a maximum length of 16 characters, with no character restrictions.

You assign password composition policies to target applications. When a user enters a password, the password is validated against the composition policy. Credential Manager also uses the password composition policy to generate random passwords.

#### WARNING

Ensure that policies meet or exceed the minimum password composition policy that is required by the target account. Also, validate that the use of special characters in the policy is allowed by the target system. The policy must follow the password requirements of the target system. If not, a password update can fail because the target system prevents the update.

Review the following topics before configuring password composition policies:

## Password Composition Rules

Password composition policies characteristics define the minimum requirements for passwords. Configurable password composition policies characteristics include:

**Remote Password Generation:** Indicates that the policy applies to remotely generated credentials. If selected, the only other rules that apply to the policy are Maximum Password Age Enforcement and Maximum Password Age Days. Other rules are hidden. Currently, only the AWS Access Credentials connector supports Remote Password Generation.

**Password Prefix:** A fixed sequence of characters that must start the password string.

**Minimum Length:** Password length must be greater than or equal to this value. Limits: 1-2048 characters.

**Maximum Length:** Password length must be less than or equal to this value. Limits: 1-2048 characters.

### NOTE

Although PAM supports a maximum password length of 2048 characters, target systems may have lower limits. For example, the maximum password length on a Linux system is 511 characters. Therefore, if you want PAM to manage accounts on a Linux system as synchronized accounts, set the **Maximum Length** value to no more than 511.

**Minimum Iterations Before Reuse:** This rule dictates a previous number of passwords are available for reuse. For example, if you enter 3, then the current password and the previous password cannot be reused. However, the third previous password and older passwords can be reused. Entering 0 means that there are no restrictions; this password can always be reused. Use this setting with the **Minimum Days Before Reuse** setting to prevent the same password from being used twice. Credential Manager checks this setting only when updating a target account password.

**Minimum Days Before Reuse:** This option prevents the reuse of any password that was used within the last specified number of days.

**Maximum Password Age Enforcement:** A password expires after this many days. The password is then considered expired. If you enable Automatically Update Expired Passwords (Settings, Credential Manager), Credential Manager updates the password. Use this setting with the **Minimum Iterations Before Reuse** setting to prevent the same password from being used twice. Credential Manager checks this setting only when updating a target account password.

**Maximum Password Age Enforcement:** This setting determines whether Credential Manager adheres to the specified password age. If disabled, the password for the target account never expires.

**Maximum Password Age Days:** This parameter specifies the maximum number of days a password is valid. The default value is 90 days. The password age is reset each time that the password is updated.

### NOTE

The **Password Expiry** date indicates the number of days from the last password update to the maximum password age. If the password expires at least one day in the future, the indicator is green. If the password expires on the current day, the indicator is yellow. If the password is already expired, the indicator is red.

**Must Contain:** This setting indicates the types of characters that a password must contain.

- At least one ASCII character set item
- Each type of character that is selected must be included in the password
- Each type of character that is not selected must be excluded in the password

**First Must Contain:** This rule specifies the first character of each password from one of the types selected. Exactly one of the options is used.

**Must Not Contain Rules:** This rule Identifies character patterns that the password must *not* contain. Options include:

- **Disallow Repeating Characters:** Do not allow any adjacent matching characters. However, duplicate characters that are not adjacent are allowed.  
Example: ABCCDECFC. The letters that are crossed out are not allowed.
- **Disallow Duplicate Characters:** Do not allow any matching characters.

Example: **ABC CDECFC**. The letters "C" after the first one are not allowed.

- **Disallow Max Class Repeat:** Do not allow consecutive characters of the same class type. If enabled, the minimum allowed is 2 and the maximum is less than the maximum password length. Example: When the Max Class Repeat is set to 2, then ABcc12#% is allowed and ABCc12#% is not allowed.
- **Characters to Exclude:** Do not allow any character from a list that you specify

In addition to the configurable options, passwords cannot begin with the following characters:

- **{n}** where *n* is any integer value; non-integer values are acceptable. For example, Credential Manager cannot manage {1}mypassword, {999}anotherpassword but can manage {104.1}okpassword.
- Passwords cannot begin or end with a space character. Credential Manager ignores a space character and does not save it.

### **Suggested Password Composition Policies**

Password composition policies must comply with password requirements of the remote applications. For the following types of targets, we suggest the following password composition policies:

- **Databases and Windows systems:**
  - Alpha and numeric characters, plus a special character, such as [!#\_-\$@\*]
  - A minimum length of six characters and a maximum length of 12 characters.
- **UNIX:** Alphabetic characters (no mixed or numeric characters) with a length of eight characters.

### **Configure Password Composition Policies**

You can create password composition policies with the UI or the CLI. Once you create password composition policies, you can then apply them to target applications.

- [Create a Password Composition Policy with the GUI](#)
- [Create a Password Composition Policy with the CLI](#)

## **Create a Password Composition Policy with the UI**

### **Create a Password Policy**

Follow these steps to create a policy in the UI:

1. Select **Credentials, Manage Targets, Password Composition Policies**. The Password Composition Policies page appears.
2. Select **Add**.
3. In the Add Password Composition Policy page, complete the fields, and select the policy rules that you want to apply. See the [descriptions of the composition rules](#).
  - Assign a unique name for the policy.
  - Select at least one of the **Must Contain**, **First Must Contain**, or **Last Must Contain** rules.
  - Do not enter same characters in **Must Contain** and **Must Not Contain** fields.
4. Select **Test**. The test lets you see the generated sample password. The test also verifies the following conditions:
  - Whether the password can be generated with the options you set
  - Whether the generated password suits your requirement
  - The complexity of the password to avoid it being figured out
5. Select **OK**.

## Automatically Update Expired Passwords

You can enable or disable the automatic updating of expired passwords globally. If it is enabled, the password for a synchronized account is automatically updated after it expires. Passwords for unsynchronized accounts remain expired until manually updated.

### Follow these steps:

1. Select **Settings, Credential Manager, General Settings**.
2. Set the **Automatically Update Expired Passwords** option. This option automatically updates synchronized accounts that have expired passwords with a new password.

See also the [Accounts with Expired Passwords](#) report.

## Create a Password Composition Policy with the CLI

To create a password composition policy from the CLI using the `addPasswordPolicy` command. You can use this command for the following tasks.

### Create a Password Composition Policy

#### Follow these steps:

1. Specify the password composition policy:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addPasswordPolicy
PasswordPolicy.name=MaximumPasswordAgePolicy
PasswordPolicy.description=PasswordCompositionPolicy
Attribute.passwordPrefix=pas
Attribute.composedOfUpperCaseCharacters=True
Attribute.composedOfLowerCaseCharacters=True
Attribute.composedOfNumericCharacters=True
Attribute.composedOfSpecialCharacters=true
Attribute.specialCharacters=!#$%()*+,-./:;=?[\\]^_{|}~
Attribute.firstCharacterUpperCase=true
Attribute.firstCharacterLowerCase=true
Attribute.firstCharacterNumeric=true
Attribute.firstCharacterSpecial=true
Attribute.firstCharacterSpecials=!#$%()*+,-./:;=?[\\]^_{|}~
Attribute.lastCharacterUpperCase=true
Attribute.lastCharacterLowerCase=true
Attribute.lastCharacterNumeric=true
Attribute.lastCharacterSpecial=true
Attribute.lastCharacterSpecials=!#$%()*+,-./:;=?[\\]^_{|}~
Attribute.mustNotContainConsecutiveDuplicateCharacters=true
Attribute.mustNotContainAnyDuplicateCharacters=true
Attribute.mustNotContainCharacters=true
Attribute.composedOfMustNotContainCharacters=XYZ
Attribute.minLength=6
Attribute.maxLength=16
Attribute.minIterationsBeforeReuse=2
Attribute.minDaysBeforeReuse=3
```

2. Enter your password at the prompt. Credential Manager returns the following XML command string:

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
```

```

<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordPolicy>
<minLength>6</minLength>
<maxLength>16</maxLength>
<minDaysBeforeReuse>3</minDaysBeforeReuse>
<minIterationsBeforeReuse>2</minIterationsBeforeReuse>
<firstCharacterSpecialCharacters>!#$%()*+,-./:;=?[\\]^_{}~</firstCharacterSpecialCharacters>
<mustNotContainCharacters>true</mustNotContainCharacters>
<passwordPrefix>pas</passwordPrefix>
<specialCharacters>!#$%()*+,-./:;=?[\\]^_{}~</specialCharacters>
<composedOfLowerCaseCharacters>true</composedOfLowerCaseCharacters>
<composedOfMustNotContainCharacters>>false</composedOfMustNotContainCharacters>
<composedOfNumericCharacters>true</composedOfNumericCharacters>
<composedOfSpecialCharacters>true</composedOfSpecialCharacters>
<composedOfUpperCaseCharacters>true</composedOfUpperCaseCharacters>
<firstCharacterLowerCase>true</firstCharacterLowerCase>
<firstCharacterNumeric>true</firstCharacterNumeric>
<firstCharacterSpecial>true</firstCharacterSpecial>
<firstCharacterUpperCase>true</firstCharacterUpperCase>
<mustNotContainDuplicateCharacters>true</mustNotContainDuplicateCharacters>
<mustNotContainRepeatingCharacters>true</mustNotContainRepeatingCharacters>
<name>NewPasswordPolicy</name>
<type>passwordPolicy</type>
<description>PasswordCompositionPolicy</description>
<ID>1006</ID>
<Attribute.composedOfNumericCharacters>true</Attribute.composedOfNumericCharacters>
<Attribute.mustNotContainCharacters>true</Attribute.mustNotContainCharacters>
<Attribute.composedOfSpecialCharacters>true</Attribute.composedOfSpecialCharacters>
<Attribute.firstCharacterNumeric>true</Attribute.firstCharacterNumeric>
<Attribute.mustNotContainAnyDuplicateCharacters>true</Attribute.mustNotContainAnyDuplicateCharacters>
<Attribute.firstCharacterSpecial>true</Attribute.firstCharacterSpecial>
<Attribute.firstCharacterSpecials>!#$%()*+,-./:;=?[\\]^_{}~</Attribute.firstCharacterSpecials>
<Attribute.firstCharacterLowerCase>true</Attribute.firstCharacterLowerCase>
<Attribute.composedOfLowerCaseCharacters>true</Attribute.composedOfLowerCaseCharacters>
<Attribute.maxLength>16</Attribute.maxLength>
<Attribute.passwordPrefix>pas</Attribute.passwordPrefix>
<Attribute.composedOfMustNotContainCharacters>>false</Attribute.composedOfMustNotContainCharacters>
<Attribute.firstCharacterUpperCase>true</Attribute.firstCharacterUpperCase>
<Attribute.minLength>6</Attribute.minLength>
<Attribute.minDaysBeforeReuse>3</Attribute.minDaysBeforeReuse>
<Attribute.specialCharacters>!#$%()*+,-./:;=?[\\]^_{}~</Attribute.specialCharacters>
<Attribute.composedOfUpperCaseCharacters>true</Attribute.composedOfUpperCaseCharacters>
<Attribute.minIterationsBeforeReuse>2</Attribute.minIterationsBeforeReuse>
<Attribute.mustNotContainConsecutiveDuplicateCharacters>true</
Attribute.mustNotContainConsecutiveDuplicateCharacters>
<createDate>Wed Nov 24 07:13:03 UTC 2010</createDate>
<createUser>admin</createUser>
<extensionType />
<hash />
<updateDate>Wed Nov 24 07:13:03 UTC 2010</updateDate>
<updateUser>admin</updateUser>
</PasswordPolicy>

```

```
</cr.result>
</CommandResult>
```

### **Set the Maximum Password Age**

The maximum password age specifies the maximum number of days a password is valid. The default value is 90 days. The password age is reset each time that the password is updated.

#### **Follow these steps:**

##### **1. Specify the new policy:**

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addPasswordPolicy
PasswordPolicy.name=MaximumPasswordAgePolicyNew
PasswordPolicy.description=PasswordCompositionPolicy
Attribute.composedOfUpperCaseCharacters=True
Attribute.composedOfLowerCaseCharacters=True
Attribute.composedOfNumericCharacters=True
Attribute.firstCharacterUpperCase=true Attribute.minLength=6
Attribute.maxLength=16 Attribute.minIterationsBeforeReuse=2
Attribute.minDaysBeforeReuse=3 Attribute.maxPasswordAge=true
Attribute.maxPasswordAge=12
```

##### **2. Enter your password at the prompt.**

Credential Manager returns the following XML command string:

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordPolicy>
<minLength>6</minLength>
<maxLength>16</maxLength>
<maxPasswordAge>0</maxPasswordAge>
<minDaysBeforeReuse>3</minDaysBeforeReuse>
<minIterationsBeforeReuse>2</minIterationsBeforeReuse>
<firstCharacterSpecialCharacters>!#$%()*+,-./:;=?@[\\]^_`{|}~&#38;
</firstCharacterSpecialCharacters>
<mustNotContainCharacters></mustNotContainCharacters>
<passwordPrefix></passwordPrefix>
<specialCharacters>!#$%()*+,-./:;=?@[\\]^_`{|}~&#38;</specialCharacters>
<composedOfLowerCaseCharacters>true</composedOfLowerCaseCharacters>
<composedOfMustNotContainCharacters>>false</composedOfMustNotContainCharacters>
<composedOfNumericCharacters>true</composedOfNumericCharacters>
<composedOfSpecialCharacters>>false</composedOfSpecialCharacters>
<composedOfUpperCaseCharacters>true</composedOfUpperCaseCharacters>
<enableMaxPasswordAge>>false</enableMaxPasswordAge>
<firstCharacterLowerCase>>false</firstCharacterLowerCase>
<firstCharacterNumeric>>false</firstCharacterNumeric>
<firstCharacterSpecial>>false</firstCharacterSpecial>
<firstCharacterUpperCase>true</firstCharacterUpperCase>
<mustNotContainDuplicateCharacters>>false</mustNotContainDuplicateCharacters>
<mustNotContainRepeatingCharacters>>false</mustNotContainRepeatingCharacters>
<name>MaximumPasswordAgePolicyNew</name>
<type>passwordPolicy</type>
```

```

<description>PasswordCompositionPolicy</description>
<ID>1004</ID>
<Attribute.composedOfNumericCharacters>true</Attribute.composedOfNumericCharacters>
<Attribute.mustNotContainCharacters></Attribute.mustNotContainCharacters>
<Attribute.composedOfSpecialCharacters>false</Attribute.composedOfSpecialCharacters>
<Attribute.firstCharacterNumeric>false</Attribute.firstCharacterNumeric>
<Attribute.maxPasswordAge>0</Attribute.maxPasswordAge>
<Attribute.enableMaxPasswordAge>false</Attribute.enableMaxPasswordAge>
<Attribute.firstCharacterSpecial>false</Attribute.firstCharacterSpecial>
<Attribute.firstCharacterSpecials>!#$%()*+,-./:;=?@[\\]^_`{|}~&#38;
</Attribute.firstCharacterSpecials>
<Attribute.mustNotContainAnyDuplicateCharacters>false
</Attribute.mustNotContainAnyDuplicateCharacters>
<Attribute.firstCharacterLowerCase>false</Attribute.firstCharacterLowerCase>
<Attribute.composedOfLowerCaseCharacters>true</Attribute.composedOfLowerCaseCharacters>
<Attribute.maxLength>16</Attribute.maxLength>
<Attribute.passwordPrefix></Attribute.passwordPrefix>
<Attribute.composedOfMustNotContainCharacters>false
</Attribute.composedOfMustNotContainCharacters>
<Attribute.firstCharacterUpperCase>true</Attribute.firstCharacterUpperCase>
<Attribute.minLength>6</Attribute.minLength>
<Attribute.minDaysBeforeReuse>3</Attribute.minDaysBeforeReuse>
<Attribute.specialCharacters>!#$%()*+,-./:;=?@[\\]^_`{|}~&#38;</Attribute.specialCharacters>
<Attribute.composedOfUpperCaseCharacters>true</Attribute.composedOfUpperCaseCharacters>
<Attribute.minIterationsBeforeReuse>2</Attribute.minIterationsBeforeReuse>
<Attribute.mustNotContainConsecutiveDuplicateCharacters>false
</Attribute.mustNotContainConsecutiveDuplicateCharacters>
<createDate>Thu Dec 01 11:17:28 UTC 2011</createDate>
<createUser>admin</createUser>
<updateDate>Thu Dec 01 11:17:28 UTC 2011</updateDate>
<updateUser>admin</updateUser>
<extensionType></extensionType>
<hash></hash>
</PasswordPolicy>
</cr.result>
</CommandResult>

```

## Configure Automatic Updating of Expired Passwords

You can enable or disable automatic updating of expired passwords globally using the `targetAccountPasswordExpirationEnabled` command. For example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty
propertyName=targetAccountPasswordExpirationEnabled propertyValues=true
```

The default value is false.

## Establish Password View Policies

Password view policies determine what actions Credential Manager takes when a password is viewed or used. In the UI, users can view target account passwords for synchronized and non-synchronized target accounts.

A password view policy can control many tasks, including:

- Automatically change the account password for synchronized accounts once it is viewed
- Automatically change the account password when a connection is ended
- Ensure that only one person at a time can view an account password
- Ensure that an account password is only revealed after a specific approver has authorized it

Each time a user views a password, Credential Manager generates a log entry. You can then view each time that a user tried to view an account password in a report.

#### NOTE

Password view policies apply only to password administration with the GUI, CLI, or Java API. Requests from A2A clients are not affected by password view policies.

The following topics describe how to work with password view policies:

- [Create a Basic Password View Policy](#)
- [Modify the Default Password View Policy](#)
- [Configure Password View Policies That Require Approval of Requests](#)
- [Require an Account Check-Out to View the Password](#)
- [Enable Email Notifications for Viewed Passwords](#)
- [Track Account Movement Across Active Directory OUs](#)
- [See a List of Password View Requests](#)

## Create a Basic Password View Policy

Each target account is associated with a password view policy, whether it is the default policy or a policy that you create. Use this procedure to create a password view policy with the UI.

To use the CLI to create a password view policy, see [Create a Password View Policy with the CLI](#).

### Configure a Password View Policy

Follow these steps:

1. Select **Credentials, Workflow, Password View Policies**. The Password View Policies page appears.
2. Select **Add**.
3. On the **Basic Info** tab, enter a policy **Name** and **Description** and specify the properties of the policy using the following controls:

#### NOTE

Use the radio buttons to display applicable and available options: either **Show All Options**, or **Show SSH Certificate Options**. Accounts that use an SSH certificate for authentication do not use a password. This means password-specific options do not apply to these accounts that use an SSH certificate for authentication.

You can still associate any password view policy option with accounts that use SSH certificates. For such accounts, viewing credentials is disabled, thus any password-view options do not apply. Also note that the options related to password rotation also do not apply. Specifically, the **Change Password On Auto Connect**, **Change Password on Connection End**, **Change Password on Session End** options will not trigger password rotation.



- **Re-authenticate for View:** If set, a dialog appears when a user tries to view a password. To continue, the user enters their password.
- **Re-authenticate for Auto-Connect:** If set, a dialog appears when a user tries to auto-connect to an application through Access. To continue, the user enters their password.
- **Reason Required for View:** If set, a dialog appears when a user tries to view an Account password. The user selects a Reason and enters a Description and Reference Code to view the password. Select the View Credential (eye icon) for an Account on the Account List page or on the Account Details page.
- **Reason Required for Auto-Connect:** If set, a dialog appears when a user tries to auto-connect. The user selects a Reason and enters an optional Description and optional Reference Code to auto-connect.
- **Change Password on View:** Viewed password on synchronized and non-synchronized accounts is automatically changed after the delay specified (in minutes) in the **Change Password Interval** field. If you also select Dual Authorization, this interval is disabled and ignored. Dual Authorization has its own Default Request Interval, which takes precedence.  
The password view policy can also require that the user check out the password to view it. For password check-out, the password is changed only when it is checked back in, regardless of the number of times the user displays the password. For compound accounts, even if only one account is accessed, the password is changed on all servers.
- **Automatic Password Change (Optional):** Set *one* of the following options to change passwords that are used in remote sessions (not "viewed" passwords):
  - **Change Password On Connection End.** A password is automatically changed when the user SSH or RDP connection to a target server ends. The connection can end because the connection times-out, the user terminates the connection, or the connection is lost. This option does not apply to "View Password."
  - **Change Password on Session End.** All passwords that are used to log in to target servers are changed when the user session in Privileged Access Manager ends. The connection can end because the user logs out, a session times out, or connectivity is lost. This option does not apply to "View Password."
- **Change Password on Auto-Connect:** If set, the password is changed a configurable number of minutes after each successful automatic connection using the credential.  
**Note:** This setting might not be suitable for environments where multiple sessions are initiated simultaneously using the same credential.
- **Password View Request Banner:** Optional. Displayed when the Reason Required for View or Reason Required for Auto-Connect is checked. If displayed, enter the text for a banner that is displayed on Password View Requests. This banner can contain information about what users need to enter in the Reason Description and Reason Code fields when they attempt to view a password for an account. You can also set this banner on the Credential Manager General Settings page. The setting in the Password View Policy takes priority over the General Setting.
- **Change Password Interval** (appears only if one or both of the **Change Password on View** or **Change Password on Auto-Connect** options are selected): Specifies an interval (in minutes) between the password view or auto-connect operation (as applicable) until Credential Manager changes the password.  
If the **Check-out/Check-in** option is also set, the Change Password Interval setting is ignored. Instead, the password is changed when the account is checked in.
- **Check-out/Check-in:** If selected, this option specifies how long Credential Manager waits (in minutes) before automatically checking in the account password.  
The Check-in/checkout interval must be less than or equal to the Dual authorization interval. When you enable check-out/check-in and dual authorization, the check-out/check-in expiry time becomes less than or equal to the dual authorization expiry time.  
For more information, see [Require an Account Check-Out to View the Password](#).
- **Exclusive Check-out On Auto Connect:** If selected, this option specifies that credentials are checked in if all connections are closed.

#### NOTE

If you select this option, all view properties and the Check-out/Check-in property are unavailable.

If Exclusive Check-out On Auto Connect is selected with service desk integration, the Reason Required for View option is selected but disabled. Even though it is selected, the functionality of view password does not work, as exclusive checkout takes precedence. Viewing of a password is disabled when the account is associated with exclusive checkout on auto connect.

4. The Dual Authorization tab is optional. **Dual Authorization** requires a person with an Approver role to grant access to the account password before a person can view the password. If you configure dual authorization, you can also enable *One-click approval*. One-click approval allows identified approvers to approve or deny the password view request without logging in to Privileged Access Manager. For more information about configuring the Dual Authorization option, see [Make a Request to View a Password](#).

**Retrospective Approval** allows immediate "break glass" access to account credentials. When these credentials are viewed, a notification is sent to administrators with an approver role for after-the-fact approval. Use this functionality to provide emergency access to accounts that would typically require *prior* authorization by an administrator with an approver role. For more information, see [Configure Password View Policies That Require Approval of Requests](#).

5. The Email Notification tab is optional. This option allows certain users to receive email notifications when another user views an account password. Emails are sent only for successful initial password view requests. See [Enable Email Notification](#) for more information.
6. The Service Desk tab is optional. To use this capability, you have to have a Service Desk integration set up already. See [Integrate with Your Service Desk Solution](#) for more information.

### **How View Policy Changes are Applied**

Any change to an existing password view policy applies to all future attempts to view a password. However, any ongoing view attempts are governed by the previous policy. For example, if you disable the Check-out/Check-in option while a password is checked out, the password remains checked out. A user checks the password back in or the check-out time expires. Therefore, if there are outstanding password view requests for an account, do not change the password view policy.

Changes that are made to the list of request approvers take effect immediately. For example, a new approver is able to receive the relevant email notification and approve or deny the request. Similarly, approver that is removed from the list can no longer receive the email or, approve or deny the request.

#### **NOTE**

For information about advanced password view policy features, see the following topics:

- [Configure Password View Policies That Require Approval of Requests](#)
- [Enable Email Notifications for Viewed Passwords](#)
- [Integrate with Your Service Desk Solution](#)

### **Create a Password View Policy with the CLI**

To create a password view policy from the CLI, use the `addPasswordViewPolicy` command.

#### **Follow these steps:**

1. Specify the Password View policy. For example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addPasswordViewPolicy
PasswordViewPolicy.name=PasswordViewPolicy
PasswordViewPolicy.description=Test
PasswordViewPolicy.changePasswordOnView=true
PasswordViewPolicy.checkinCheckoutRequired=true
PasswordViewPolicy.authenticationRequired =true
PasswordViewPolicy.checkinCheckoutInterval=60
PasswordViewPolicy.dualAuthorization=true
```

```

PasswordViewPolicy.passwordViewRequestMaxDays=7
PasswordViewPolicy.passwordViewRequestMaxInterval=60
PasswordViewPolicy.dualAuthorizationInterval=60
PasswordViewPolicy.changePasswordOnConnectionEnd=true
PasswordViewPolicy.changePasswordOnSessionEnd=false
PasswordViewPolicy.enableOneClickApproval=true
PasswordViewPolicy.approvers=approver1,approver2
PasswordViewPolicy.emailNotificationRequired=true
PasswordViewPolicy.emailNotificationToDualAuthApprovers=false
PasswordViewPolicy.emailNotificationToActiveUsers=true
PasswordViewPolicy.emailNotificationUsers=user1,user2

```

## 2. Enter your password at the prompt.

Credential Manager returns an XML command string. For example:

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewPolicy>
<name>PasswordViewPolicy</name>
<readOnly>>false</readOnly>
<description>Test</description>
<enableOneClickApproval>true</enableOneClickApproval>
<changePasswordOnView>true</changePasswordOnView>
<emailNotificationRequired>true</emailNotificationRequired>
<dualAuthorizationRequired>true</dualAuthorizationRequired>
<passwordViewRequestMaxDays>14</passwordViewRequestMaxDays>
<passwordViewRequestMaxInterval>60</passwordViewRequestMaxInterval>
<dualAuthorizationInterval>60</dualAuthorizationInterval>
<changePasswordOnConnectionEnd>true</changePasswordOnConnectionEnd>
<changePasswordOnSessionEnd>>false</changePasswordOnSessionEnd>
<approvers>approver1,approver2</approvers>
<approverIDs>[]</approverIDs>
<emailNotificationUserIDs>[]</emailNotificationUserIDs>
<checkinCheckoutRequired>true</checkinCheckoutRequired>
<checkinCheckoutInterval>60</checkinCheckoutInterval>
<passwordChangeInterval>60</passwordChangeInterval>
<emailNotificationForDualAuthApprovers>>false</emailNotificationForDualAuthApprovers>
<authenticationRequired>true</authenticationRequired>
<emailNotificationForActiveUsers>true</emailNotificationForActiveUsers>
<emailNotificationUsers>user1,user2</emailNotificationUsers>
<ID>1016</ID>
<createDate>Wed Nov 17 07:46:45 UTC 2010</createDate>
<createUser>admin</createUser>
<extensionType />
<hash>u09WfJd7m5RNv2N/3ZgIqVGU00M=</hash>
<updateDate>Wed Nov 17 07:46:45 UTC 2010</updateDate>
<updateUser>admin</updateUser>
</PasswordViewPolicy>
</cr.result>
</CommandResult>

```

The previous example creates a policy that is named `PasswordViewPolicy`. This new policy specifies:

- An account password must be changed once it is viewed.
- Only one person at a time can view an account password.
- The person must authenticate before viewing an account password.
- After a password is checked out, a password is automatically checked in after 60 minutes.
- After a connection is established, that password is automatically changed after that session is closed or times out.
- When the password is viewed, an email must be sent to the list of identified approver.
- The email sent to list of approvers must contain two URLs (one to approve and another to deny the password view request).
- When the password is viewed, an email is sent to the list of identified users.

### **Customize Reasons for Viewing Password**

Use the `setPasswordViewReasons` CLI command to customize the list of reasons for viewing a password that is displayed to GUI users. See [setPasswordViewReasons](#) for details.

## **Modify the Default Password View Policy**

You can edit the default password view policy to customize it for your requirements. The customized policy becomes the default policy.

### **NOTE**

Do not change the name of the default policy. Leave the name as **Default**.

Use the following procedure to modify the default password view policy.

### **Follow these steps:**

1. Select **Credentials, Workflow, Password View Policies**.
2. Select the **Default** option and select **Update**.
3. Modify the options on the various tabs, as required.  
For more information about the settings, see [Create a Basic Password View Policy](#).
4. select **OK**.

## **Configure Password View Policies That Require Approval of Requests**

To require that password view requests be approved by another administrator, enable one of the following options in the Password View Policy:

- **Dual Authorization:** Requires an administrator with an *approver* role to authorize access *before* the requester can access account credentials.
- **Retrospective Approval:** Provides immediate access to account credentials and sends a notification to administrators with an approver role for retrospective (after-the-fact) approval. Use this functionality (often referred to as "break glass") to provide emergency access to accounts that would typically require *prior* authorization by an administrator with an approver role.

This content contains the following information:

To configure dual authorization or retrospective approval using the CLI, see [Password View Requests in the CLI](#).

### **Who Can Be An Approver?**

Dual authorization and retrospective approval require an approver to allow, deny, and delete password view requests. For a user to become an approver, that user must meet two criteria:

- The user must have a role with the **credentialsManage** privilege. Roles with this privilege are:

- Global Administrator
- Password Manager
- Operational Administrator

For more about roles and privileges, see [Identify Desired User Roles](#).

- The user must belong to a Credential Manager group that includes a Credential Manager role with the following privileges:
  - Update Password View Request Status
  - List Password View Request Summary By Approver

For example, the System Admin Group is a Credential Manager group with the necessary privileges.

To see a list of Credential Manager roles in each group, select **Credentials, Manage Credential Groups** then double-click a role in the list and view the selected privileges for that role.

### **Configure a Password View Policy That Requires Dual Authorization**

Configure dual authorization to require an administrator with an *approver* role to authorize access *before* the requester can access account credentials. Credential Manager sends an email to the requesters notifying them of the password view request decision. If the request is approved, the requester can view the password.

Enable and configure dual authorization using the following procedure.

#### **Follow these steps:**

1. Go to **Credentials, Workflow, Password View Policies**.
2. On the **Dual Authorization** tab, select the **Dual Authorization** checkbox.
3. Set the time period for View Password requests.
  - **Request must be within:** Specifies the time frame within which the password view can be requested. The default value is 14 days.
  - **Default Request Interval:** Specifies the default interval in minutes to view the password, if applicable. The default value is 60 minutes. When a user requests a password, the time between the **Request Password From** and **Request Password To** fields is set to the default request interval.
  - **Maximum Request Interval:** Specifies the maximum interval in minutes, up to which the password can be viewed, if applicable. The default value is 60 minutes.

When users request password viewing, it is for a specific time period. For example, August 8 from 9:00 to 11:00. Specify the time zone in **Global Settings, Default Preferences**.

#### **NOTE**

This time period defines when a user can retrieve and view a password. The View Password function does not initiate session management.

4. (Optional) Select **Enable One Click Approval**.  
If selected, this option allows specified approvers to approve or deny the password view request without logging in to Credential Manager. If enabled, approvers are sent an email notification whenever someone attempts to view the password. The email notification all the standard details and a URL that approves the request and a URL that denies the request. The approver can select the approve or deny URL directly from the email without logging in to PAM. If One Click Approval is *not* enabled, each approver still receives an email, but without the URLs. Instead, the approver must log in to view a list of pending requests, which are approved, denied, or expired.
5. From the **Available Approvers** list, select users and move them to the **Selected Approvers** list.
6. Select **OK**.

When a user or administrator makes a request to view the password, Credential Manager automatically sends an email notification to the approvers for that account. The notification includes the following request details:

- Name of the user submitting the request
- Account name for the requested password view
- Requested account target application
- Requested account target server
- Password view reason
- Requested timeframe (in UTC)

### **Configure a Password View Policy That Requires Retrospective Approval**

Configure retrospective approval to allow immediate emergency "break glass" access to account credentials and send a notification to administrators with an *approver* role for retrospective (after-the-fact) approval.

#### **Follow these steps:**

1. Go to **Credentials, Workflow, Password View Policies**.
2. On the **Dual Authorization** tab, select the **Retrospective Approval** checkbox.
3. (Optional) Select **Enable One Click Approval**.  
If selected, this option allows specified approvers to approve or deny the password view request without logging in to Credential Manager. If enabled, approvers are sent an email notification whenever someone attempts to view the password. The email notification all the standard details and a URL that approves the request and a URL that denies the request. The approver can select the approve or deny URL directly from the email without logging in to PAM. If One Click Approval is *not* enabled, each approver still receives an email, but without the URLs. Instead, the approver must log in to view a list of pending requests, which are approved, denied, or expired.
4. From the **Available Approvers** list, select users and move them to the **Selected Approvers** list.
5. Select **OK**.

When a user or administrator makes a request to view the password, a dialog informs them that their request is for emergency access and requires retrospective approval. If they decide to proceed, Credential Manager automatically sends an email notification and adds the request to the **My Password View Approvals** list of assigned approvers. However, because the credentials have already been accessed, the only effect of approval or denial is how the request is audited in the session logs.

For further information, see the following content:

- [Creating Custom Approvers \(Optional\)](#)
- [Process View Requests as an Approver](#)
- [View Dual Authorization Requests in the CLI](#)
- [View Retrospective Approval Requests in the CLI](#)

### **Creating Custom Approvers (Optional)**

If dual authorization is enabled, a user who is designated as an approver must grant permission to view the password. A set of preconfigured Credential Manager groups exists, which have roles with the necessary privileges to be an approver. For example, the System Admin Group contains the System Admin role, which has the required privileges for authorizing password views.

You can create a role and can add it to a Credential Manager group. Any user that is a part of the group with the new role can act as an approver.

The new role must have the following permissions:

- List Password View Request Summary By Approver
- Update Password View Request Status

In addition, an approver must have a valid email address. Their user group must also be able to access the accounts they are approving.

To create an approver role, see [Add or Modify Credential Manager Roles](#).

## Process Password View Requests as an Approver

This content describes how to process dual authorization and retrospective approval password view requests.

### Process Dual Authorization Requests

As an approver for a [dual authorization password view policy](#), you can grant, deny, or expire a password view request. You can act on a specific request only once.

When the password view request exceeds the date and time in the request, the request status changes automatically. For example, a password view request start date and time are 2012-11-19 18:06 and the end date and time is 2012-11-19 19:06. After 2012-11-19 19:06, the status of the request that is yet pending changes to Expired. The status of the request that is approved or denied changes to Approved, Expired, or Denied. The status of the request that is checked in or checked out changes to Checked In or Checked Out.

The following methods are different ways to view requests:

#### *Handle Requests from My Approval List*

##### Follow these steps:

1. Navigate to **Credentials, Workflow, My Approvals**. A list of requests appears.
2. Select a specific pending password view request and select the **VIEW** button. The **Password View Request Details** pane appears.
3. After reviewing the reason details in the email, select the appropriate option to approve, deny, or expire the request.

#### **NOTE**

You can also select multiple password view requests and then select **Approve All** or **Deny All**.

#### *Approve or Deny Requests from the Target Accounts Panel*

After you receive an email notification of a password view request, review the details in the email. Then, approve or deny the request from the Current Requests section on the **Target Accounts** panel.

#### **NOTE**

You cannot expire a password from the **Current Requests** section. You must select the entry and must select **Expire** from the **Password View Request Details** panel.

##### Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**. The **Account List** panel appears with a list of current requests.
2. Take one of the following actions in the **Current Requests** section:
  - Select the green Thumbs Up icon under the **Action** column for the appropriate account.
  - Select the red Thumbs Down icon under the **Action** column for the account.
 The **Password View Request Approval** pop-up appears.
3. Select **Approve** or **Deny**.
4. Select the reason to approve the request from the drop-down list.
5. (Optional) Enter the reason description.
6. Select **Save**.
7. When you are prompted to confirm the approval, select **Yes**.



### ***Grant or Deny a One-Click Approval Request***

A password view policy might be enabled for dual authorization with one-click approval. When a person attempts to view the account password with these features enabled, Credential Manager sends an email to the approver. The approver can approve or deny the request directly from the received email without logging in to the appliance.

#### **NOTE**

The contents of the email can differ based on the email template configuration. See [Configure the Email Server and Email Templates](#).

The approver can review the reason details in the email then approve or deny the request by:

- Clicking the URL given for approving the password view request. The password view request status is updated to Approved. A web page appears with the approval confirmation message.
- Clicking the URL given for denying the password view request. The password view request status is updated to Denied. A web page appears with the rejection message.

Under the following conditions, the approver might be redirected to an error page:

- The approver is invalid or expired.
- The password view request is invalid or expired.
- The status is invalid.
- The password view request is already approved or denied.

### **Process Retrospective Approval Requests**

As an approver for a [retrospective approval password view policy](#), you can retrospectively acknowledge or decline a password view request. You can act on a specific request only once.

#### **Follow these steps:**

1. Navigate to **Credentials, Workflow, My Approvals**. A list of requests appears.
2. Select a specific pending password view request and select the **VIEW** button.  
The **Password View Request Details** pane appears.
3. After reviewing the reason details in the email, select the appropriate option to acknowledge or decline the request.

#### **NOTE**

You can also select multiple password view requests and then select **Acknowledge All** or **Decline All**.

### **Identify Extended Timeout Requirements in Password View Requests with Extended Timeout**

As an approver, you can see the connection idle timeout value that is associated with a password view request in the following locations:

- The **Timeout** column on the **My Password View Approvals** panel (**Credentials, Workflow, My Approvals**).
- The **Connection Idle Time (Minutes)** entry on the **Password View Request Details** pane

To identify a password view request seeking an [extended timeout](#), look for a value more than the default **Connection Idle Timeout** specified in the [Global Settings](#).

### **Delete a View Request Using the UI**

All password view requests with status Approved, Denied, Pending, Expired, Acknowledged, or Denied are available in the My Approval List. Any password view request that is not required can be deleted from the My Approval List with the UI.

Use the following procedure to delete a request using the UI My Approval List.



**Follow these steps:**

1. Go to **Credentials, Workflow, My Approvals**. The My Approval List Panel appears.
2. Select the check box corresponding the password view requests to be deleted. Select **Delete**.
3. When you are prompted to confirm the deletion, select **OK**.

**Delete View Requests Automatically**

You can automate the removal of password view requests using the **Password View Request Delete Interval Days** setting. For example, if you set the value of the interval for two days, the requests are deleted automatically from the list after every two days.

**Follow these steps to set the delete interval:**

1. Go to **Settings, Credential Manager, General Settings**.
2. In the **Password View Request Delete Interval Days** field, enter the number of days you want view requests removed.
3. Select **Save**.

**View Dual Authorization Requests in the CLI****Make a Request to View a Password Using the CLI**

If the password view policy specifies dual authorization, requests to view a password are sent to the approver.

In such cases, the XML command string that is returned from the operation:

- Contains a status code of 400, indicating successful operation
- Excludes all account details except a warning message indicating that the request has been forwarded for processing

**Follow these steps:**

1. Search target accounts to retrieve the target account ID:

Windows:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount ^
TargetAccount.userName=dualaccount
```

Linux:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount \
TargetAccount.userName=dualaccount
```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **1005**.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<TargetAccount>
<privileged>true</privileged>
<aliases />
<password>{1}3d2876d75f730fcf7b00f974816aa97b</password>
<lastUsed />
<passwordViewPolicyID>1013</passwordViewPolicyID>
<accessType />
<cacheBehavior>useCacheFirst</cacheBehavior>
<cacheDuration>30</cacheDuration>
<compoundServerList>[]</compoundServerList>
```

```

<lastVerified />
<lastViewed />
<targetApplicationID>1001</targetApplicationID>
<userName>dualaccountnew</userName>
<compoundAccount>false</compoundAccount>
<passwordVerified>false</passwordVerified>
<synchronize>false</synchronize>
<targetApplication />
<cacheAllow>true</cacheAllow>
<targetServerAlias />
<ID>1005</ID>
<Attribute.extensionType>mssql</Attribute.extensionType>
<Attribute.useOtherAccountToChangePassword>false
</Attribute.useOtherAccountToChangePassword>
<Attribute.cspm_serverkeyid>1</Attribute.cspm_serverkeyid>
<Attribute.descriptor1 />
<Attribute.descriptor2 />
<createDate>Tue Nov 16 12:44:50 UTC 2010</createDate>
<createUser>admin</createUser>
<extensionType>mssql</extensionType>
<hash>FIRqOhKpXVlsglrsroJzlyHmzH4=</hash>
<updateDate>Tue Nov 16 12:44:50 UTC 2010</updateDate>
<updateUser>admin</updateUser>
</TargetAccount>
</cr.result>
</CommandResult>

```

### 3. View the password. Use the ID provided by the output of the previous command:

Windows:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword ^
TargetAccount.ID=1005 reason=Poweroutagereason reasonDetails=Recover Tuesday pm ^
PasswordViewRequest.requestPeriodStart="2010-11-16 16:58" ^
PasswordViewRequest.requestPeriodEnd="2010-11-16 17:05"

```

Linux:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword \
TargetAccount.ID=1005 reason=Poweroutagereason reasonDetails=Recover Tuesday pm \
PasswordViewRequest.requestPeriodStart="2010-11-16 16:58" \
PasswordViewRequest.requestPeriodEnd="2010-11-16 17:05"

```

### 4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.warningCode>4625</cr.warningCode>
<cr.warningMessage>This account has dual authorization enabled.
A request to view the password has been e-mailed to the approvers of this account on your behalf.
</cr.warningMessage>
</CommandResult>

```

## **Grant, Deny, or Expire a Request Using the CLI**

Use the following procedure to approve or deny a password view request from the CLI using the `updatePasswordViewRequestStatus` command.

### **Follow these steps:**

1. Search target accounts to retrieve the target account ID:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchPasswordViewRequestByApprover
```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **4**.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewRequest>
<status>1</status>
<targetAccountID>1</targetAccountID>
<startDate/>
<endDate/>
<requestorID>3</requestorID>
<approverID>-1</approverID>
<ID>4</ID>
<createDate>Wed Sep 10 14:42:20 UTC 2008</createDate>
<createUser>req1</createUser>
<hash>RLMwHaMdENV9mlFnoSsoSOJezJw=</hash>
<updateDate>Wed Sep 10 15:42:20 UTC 2008</updateDate>
<updateUser>req1</updateUser>
<extensionType/>
</PasswordViewRequest>
</cr.result>
</CommandResult>
```

3. Change the status of the password view request to approved or denied. Use the ID provided by the output of the previous command:

Windows:

```
capam_command adminUserID=admin capam=mycompany.com ^
cmdName=updatePasswordViewRequestStatus PasswordViewRequest.ID=4 ^
PasswordViewRequest.status=approved
```

Linux:

```
capam_command adminUserID=admin capam=mycompany.com \
cmdName=updatePasswordViewRequestStatus PasswordViewRequest.ID=4 \
PasswordViewRequest.status=approved
```

4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewRequest>
<status>1</status>
<targetAccountID>1</targetAccountID>
```

```

<startDate>Wed Sep 10 15:47:00 UTC 2008</startDate>
<endDate>Wed Sep 10 16:02:00 UTC 2008</endDate>
<requestorID>3</requestorID>
<approverID>1</approverID>
<ID>1</ID>
<createDate>Wed Sep 10 14:42:20 UTC 2008</createDate>
<createUser>reql</createUser>
<hash>Yc5gR/IpPVh8evYKGipQYa9AGXU=</hash>
<updateDate>Wed Sep 10 15:47:09 UTC 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType/>
</PasswordViewRequest>
</cr.result>

```

Use the following procedure to expire a password view request from the CLI using the `expirePasswordViewRequestCmd` command.

### Follow these steps:

1. Search target accounts to retrieve the target account ID:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchPasswordViewRequestByApprover
```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is 4.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewRequest>
<status>1</status>
<targetAccountID>1</targetAccountID>
<startDate/>
<endDate/>
<requestorID>3</requestorID>
<approverID>-1</approverID>
<ID>4</ID>
<createDate>Wed Sep 10 14:42:20 UTC 2008</createDate>
<createUser>reql</createUser>
<hash>RLMwHaMdENV9mlFnoSsoSOJezJw=</hash>
<updateDate>Wed Sep 10 15:42:20 UTC 2008</updateDate>
<updateUser>reql</updateUser>
<extensionType/>
</PasswordViewRequest>
</cr.result>
</CommandResult>

```

3. Change the status of the password view request to approved or denied. Use the ID provided by the output of the previous command:

Windows:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=expirePasswordViewRequestCmd ^
PasswordViewRequest.ID=4
```

Linux:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=expirePasswordViewRequestCmd \
PasswordViewRequest.ID=4
```

#### 4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
</cr.result>
```

### **Update the Approval or Denial Reasons for a Request Using the CLI**

The reasons to be populated in the Reason drop-down list while approving or denying the password view request using the GUI, can be updated using the `setSystemProperty` command.

To update the list of approval reasons, use:

```
Windows:
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordApprovalReasons ^
propertyValues=reason1|reason2
Linux:
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordApprovalReasons \
propertyValues=reason1|reason2
```

To update the list of denial reasons, use:

```
Windows:
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordDenialReasons ^
propertyValues=reason1|reason2
Linux:
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordDenialReasons \
propertyValues=reason1|reason2
```

The `|` character delimits multiple reasons.

### **View Retrospective Approval Requests in the CLI**

#### **Make a Request to View a Password Using the CLI**

If the password view policy specifies retrospective approval, requests to view a password are sent to the approver.

In such cases, the XML command string that is returned from the operation:

- Contains a status code of 400, indicating successful operation
- Excludes all account details except a warning message indicating that the request has been forwarded for processing

#### **Follow these steps:**

##### 1. Search target accounts to retrieve the target account ID:

```
Windows:
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount ^
TargetAccount.userName=breakglassaccount
Linux:
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount \
TargetAccount.userName=breakglassaccount
```

##### 2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **1005**.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<TargetAccount>
<privileged>true</privileged>
<aliases />
<password>{1}3d2876d75f730fcf7b00f974816aa97b</password>
<lastUsed />
<passwordViewPolicyID>1013</passwordViewPolicyID>
<accessType />
<cacheBehavior>useCacheFirst</cacheBehavior>
<cacheDuration>30</cacheDuration>
<compoundServerList>[]</compoundServerList>
<lastVerified />
<lastViewed />
<targetApplicationID>1001</targetApplicationID>
<userName>dualaccountnew</userName>
<compoundAccount>false</compoundAccount>
<passwordVerified>false</passwordVerified>
<synchronize>false</synchronize>
<targetApplication />
<cacheAllow>true</cacheAllow>
<targetServerAlias />
<ID>1005</ID>
<Attribute.extensionType>mssql</Attribute.extensionType>
<Attribute.useOtherAccountToChangePassword>false
</Attribute.useOtherAccountToChangePassword>
<Attribute.cspm_serverkeyid>1</Attribute.cspm_serverkeyid>
<Attribute.descriptor1 />
<Attribute.descriptor2 />
<createDate>Tue Nov 16 12:44:50 UTC 2010</createDate>
<createUser>admin</createUser>
<extensionType>mssql</extensionType>
<hash>FIRqOhKpXVlsglrsroJzlyHmzH4=</hash>
<updateDate>Tue Nov 16 12:44:50 UTC 2010</updateDate>
<updateUser>admin</updateUser>
</TargetAccount>
</cr.result>
</CommandResult>

```

### 3. View the password. Use the ID provided by the output of the previous command:

Windows:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword ^
TargetAccount.ID=1005 reason=Poweroutagereason reasonDetails=Recover Tuesday pm ^
PasswordViewRequest.requestPeriodStart="2010-11-16 16:58" ^
PasswordViewRequest.requestPeriodEnd="2010-11-16 17:05"

```

Linux:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword \
TargetAccount.ID=1005 reason=Poweroutagereason reasonDetails=Recover Tuesday pm \
PasswordViewRequest.requestPeriodStart="2010-11-16 16:58" \
PasswordViewRequest.requestPeriodEnd="2010-11-16 17:05"

```

#### 4. Enter your password at the prompt.

Credential Manager immediately returns the requested password in the following XML command string. Internally, a retrospective approval request is generated and sent to the account owner for retrospective approval.

```
<CommandResult>
  <cr.itemNumber>0</cr.itemNumber>
  <cr.statusCode>400</cr.statusCode>
  <cr.statusDescription>Success.</cr.statusDescription>
  <cr.result>
    <TargetAccount>
      <userName>qa</userName>
      <targetApplicationID>1007</targetApplicationID>
      <accessType></accessType>
      <targetApplication></targetApplication>
      <passwordVerified>true</passwordVerified>
      <compoundServerList>[]</compoundServerList>
      <synchronize>true</synchronize>
      <ownerUserID>-1</ownerUserID>
      <compoundAccount>false</compoundAccount>
      <cacheBehavior>useCacheFirst</cacheBehavior>
      <cacheDuration>30</cacheDuration>
      <compoundServerIDs>null</compoundServerIDs>
      <passwordViewPolicyID>1001</passwordViewPolicyID>
      <cacheAllow>true</cacheAllow>
      <lastUsed>Tue Nov 27 17:34:00 UTC 2018</lastUsed>
      <serverKeyId>-1</serverKeyId>
      <cacheBehaviorInt>1</cacheBehaviorInt>
      <targetServerAlias></targetServerAlias>
      <lastVerified>Fri Nov 09 16:34:10 UTC 2018</lastVerified>
      <lastViewed>Tue Nov 27 17:34:00 UTC 2018</lastViewed>
      <aliases></aliases>
      <password>n3wp@ss</password>
      <privileged>true</privileged>
      <Attribute.keyOptions></Attribute.keyOptions>
      <Attribute.verifyThroughOtherAccount>false</Attribute.verifyThroughOtherAccount>
      <Attribute.discoveryAllowed>false</Attribute.discoveryAllowed>
      <Attribute.publicKey></Attribute.publicKey>
      <Attribute.privateKey></Attribute.privateKey>
      <Attribute.protocol>SSH2_PASSWORD_AUTH</Attribute.protocol>
      <Attribute.otherAccount></Attribute.otherAccount>
      <Attribute.descriptor2></Attribute.descriptor2>
      <Attribute.discoveryGlobal>false</Attribute.discoveryGlobal>
      <Attribute.descriptor1></Attribute.descriptor1>
      <Attribute.extensionType>unixII</Attribute.extensionType>
      <Attribute.useOtherAccountToChangePassword>false</Attribute.useOtherAccountToChangePassword>
      <Attribute.passphrase></Attribute.passphrase>
      <Attribute.passwordChangeMethod>DO_NOT_USE_SUDO</Attribute.passwordChangeMethod>
      <createTime>1541781247000</createTime>
      <createDate>Fri Nov 09 16:34:07 UTC 2018</createDate>
      <extensionType>unixII</extensionType>
      <updateDate>Fri Nov 09 16:43:30 UTC 2018</updateDate>
      <createUser>super</createUser>
      <updateTime>1541781810000</updateTime>
      <updateUser>super</updateUser>
    </TargetAccount>
  </cr.result>
</CommandResult>
```

```

<hash>gSRczWKdl0hlGnCf0szsI5kSKbY=</hash>
<ID>1005</ID>
</TargetAccount>
</cr.result>
</CommandResult>

```

### **Acknowledge or Decline a Request Using the CLI**

Use the following procedure to acknowledge or decline a password view request from the CLI using the `updatePasswordViewRequestStatus` command.

#### **Follow these steps:**

1. Search target accounts to retrieve the target account ID:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchPasswordViewRequestByApprover
```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **4**.

```

<CommandResult>
  <cr.itemNumber>0</cr.itemNumber>
  <cr.statusCode>400</cr.statusCode>
  <cr.statusDescription>Success.</cr.statusDescription>
  <cr.result>
    <PasswordViewRequest>
      <endDate>Fri Nov 30 22:21:00 UTC 2018</endDate>
      <startDate>Fri Nov 30 22:21:00 UTC 2018</startDate>
      <ssoType></ssoType>
      <requestorID>1000</requestorID>
      <targetAccountID>1005</targetAccountID>
      <approverID>-1</approverID>
      <referenceCode></referenceCode>
      <reasonDescription>view</reasonDescription>
      <approvalReason></approvalReason>
      <approvalReasonDescription></approvalReasonDescription>
      <approverIPAddress></approverIPAddress>
      <viewStatus>1</viewStatus>
      <reason>view</reason>
      <status>11</status>
      <createTime>1543616479000</createTime>
      <createDate>Fri Nov 30 22:21:19 UTC 2018</createDate>
      <extensionType></extensionType>
      <updateDate>Fri Nov 30 22:21:19 UTC 2018</updateDate>
      <createUser>super</createUser>
      <updateTime>1543616479000</updateTime>
      <updateUser>super</updateUser>
      <hash>XtwwNcuGn4807UrSSekcq5g3Mlo=</hash>
      <ID>1059</ID>
    </PasswordViewRequest>
  </cr.result>
</CommandResult>

```

3. Change the status of the password view request to acknowledged or declined. Use the ID provided by the output of the previous command:

```

Windows:
capam_command adminUserID=admin capam=mycompany.com ^

```



```
cmdName=updatePasswordViewRequestStatus PasswordViewRequest.ID=4 ^
PasswordViewRequest.status=acknowledged
Linux:
capam_command adminUserID=admin capam=mycompany.com \
cmdName=updatePasswordViewRequestStatus PasswordViewRequest.ID=4 \
PasswordViewRequest.status=acknowledged
```

#### 4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```
<CommandResult>
  <cr.itemNumber>0</cr.itemNumber>
  <cr.statusCode>400</cr.statusCode>
  <cr.statusDescription>Success.</cr.statusDescription>
  <cr.result>
    <PasswordViewRequest>
      <endDate>Fri Nov 30 22:21:00 UTC 2018</endDate>
      <startDate>Fri Nov 30 22:21:00 UTC 2018</startDate>
      <ssoType></ssoType>
      <requestorID>1000</requestorID>
      <targetAccountID>1005</targetAccountID>
      <approverID>1000</approverID>
      <referenceCode></referenceCode>
      <reasonDescription>view</reasonDescription>
      <approvalReason></approvalReason>
      <approvalReasonDescription></approvalReasonDescription>
      <approverIPAddress></approverIPAddress>
      <viewStatus>1</viewStatus>
      <reason>view</reason>
      <status>9</status>
      <createTime>1543616479000</createTime>
      <createDate>Fri Nov 30 22:21:19 UTC 2018</createDate>
      <extensionType></extensionType>
      <updateDate>Fri Nov 30 22:36:23 UTC 2018</updateDate>
      <createUser>super</createUser>
      <updateTime>1543617383416</updateTime>
      <updateUser>super</updateUser>
      <hash>ouVRldocSDru0WMQ1Q/cXDmyRfg=</hash>
      <ID>1059</ID>
    </PasswordViewRequest>
  </cr.result>
</CommandResult>
```

### **Update the Acknowledge or Decline Reasons for a Request Using the CLI**

The reasons to be populated in the Reason drop-down list while acknowledging or denying the password view request using the GUI, can be updated using the `setSystemProperty` command.

To update the list of acknowledgement reasons, use:

```
Windows:
cspmservice_admin cmdName=setSystemProperty propertyName=ViewPasswordAcknowledgeReasons ^
propertyValues=reason1
Linux:
cspmservice_admin cmdName=setSystemProperty propertyName=ViewPasswordAcknowledgeReasons \
```

```
propertyValues=reason1
```

To update the list of denial reasons, use:

Windows:

```
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordDeclineReasons ^
propertyValues=reason1|reason2
```

Linux:

```
cspmserver_admin cmdName=setSystemProperty propertyName=viewPasswordDeclineReasons \
propertyValues=reason1|reason2
```

The | character delimits multiple reasons.

## Require an Account Check-Out to View the Password

If an account has a Check-out/Check-in view policy, the account must be checked out to view the password. The person then has exclusive access to the password. While it is checked out, other persons cannot view the password nor can they change any aspect of the account in any way. Once the password is checked back in to Credential Manager, others can view it and can update it.

The Check-out/Check-in policy can have a time interval, after which the account is automatically checked back in.

Sometimes an administrator needs immediate access to a password that is checked out. The administrator can remove the restriction on the account by checking in the account on behalf of another user. By default, only the administrator role has permission to force a check-in operation. If necessary, you can configure other roles with this permission.

This topic describes the following procedures:

For the equivalent procedures using the CLI, see [Require a Password Check Out and Check using the CLI](#).

### Check Out a Password Using the UI

Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the blue View icon (which resembles an eye) in the **Action** column of the Account for which you want to request authorization. A Show Password pop-up window appears, prompting you for your password and the reasons for viewing the target password.
3. Enter your (Credential Manager administrator) password.

#### **NOTE**

The password field is displayed if the target account is authenticated.

4. Select your **Reason** for viewing the (target account) password.
5. (Optional) Enter the **Reason Description**.
6. Select **View**.  
The GUI displays the account User ID and the password. The GUI also notifies you that the account is checked out.
7. Select **OK**.

### Determine Who Has a Password Checked Out

Use the following procedure to find out how has a password that is checked out.

Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. For the appropriate entry in the Target Accounts list, select the blue Checkout icon (which resembles an eye with an X across it) located in the Action column. A dialog appears showing who has checked out the password.

The Reference Code is shown only if the requestor has entered the reference code in View Account Password Request screen before viewing the account password.

### **Check In a Password Using the UI**

When you check out a password, no other user can view the password or can change the account until you select it back in again. Checking in the password removes this restriction and frees the account for use by others. In emergency situations, an administrator can check in a password on behalf of another user.

#### **NOTE**

Checking in passwords does not affect open access sessions. Users currently in active access sessions will remain logged in regardless of the password being checked in.

You can check in an account password from the following GUI locations:

- Credentials, Manage Targets, Accounts
- Credentials, Workflow, My Requests
- Access screen

Use the following procedure to check in a password from the **Credentials, Manage Targets, Accounts** screen.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. For the account password to be checked in, select the Check-In icon (a black right-facing arrow inside a box). The icon is in the Action column.  
A message confirms that the password has been checked in.

Use the following procedure to check in a password from the **Credentials, Workflow, My Requests** screen.

#### **Follow these steps:**

1. Select **Credentials, Workflow, My Requests**
2. Select the entry for the account (with status "Checked Out") whose password you want to check in and select **View**. The Password View Request Details screen appears.
3. In the Password View Request Details dialog, select **CHECK IN**.  
A message confirms that the password has been checked in.

Use the following procedure to check in a password from the **Access** screen.

#### **Follow these steps:**

1. If you are logged in as an administrator, select **Access** from the main menu. If you are not an administrator, the home screen *is* the Access screen (though it is not labeled).  
A list of checked out passwords is presented at the top of the screen.

#### **NOTE**

If you are not an administrator, you might need to log out and log back in again before checked-out passwords are visible.

2. Select **Check In** in the right-hand column of the password line item.

### **Force a Password Check In Using the GUI**

When an account password is checked out, other users cannot view the password nor can they change the account. Use this procedure to force a check-in of an account password on behalf of another user.

**NOTE**

Checking in passwords does not affect open access sessions. Users currently in active access sessions will remain logged in regardless of the password being checked in.

**NOTE**

When you perform a forced check in, any required activities that are associated with that operation also occur, for example, an update of the account password.

The administrator can check in an account on behalf of another user from the following screens:

- **Credentials, Manage Targets, Accounts**
- **Credentials, Workflow, All Requests**

User the following procedure to check in a password using the **Credentials, Manage Targets, Accounts** screen.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. For the password to be checked in, select the Check-In icon (black right-facing arrow inside a box). The icon is in the Action column.  
A message confirms that the password has been checked in.

Use the following procedure to check in a password using the **Credentials, Workflow, All Requests** screen.

**Follow these steps:**

1. Select **Credentials, Workflow, All Requests**.
2. Select the account (with status "Checked Out") for which you want to view check out details and select **View**. The Password View Request Details screen appears.
3. Select the **FORCE CHECK-IN** button.  
The account password is checked in.

**Check Out An Account Using the CLI**

You can use the CLI to require that an account is checked out to view the password.

**Check Out an Account to View the Password**

Using the CLI, you can require an account check-out using the `addPasswordViewPolicy` command and the parameter `PasswordViewPolicy.checkinCheckoutRequired=true`.

Example:

```
capam_command capam=capamServer adminUserID=admin cmdName=addPasswordViewPolicy
PasswordViewPolicy.name=restrictedAccounts PasswordViewPolicy.changePasswordOnView=true
PasswordViewPolicy.checkinCheckoutRequired=true
PasswordViewPolicy.checkinCheckoutInterval=240
```

When a user views the password, message displays indicating that the account is checked out.

Use the following procedure to view an account password from the CLI.

**Follow these steps:**

1. Search target accounts to retrieve the target account ID:  

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount
TargetAccount.userName=account1
```

## 2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **1**.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 UTC 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 UTC 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>l4adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>Mon Nov 12 15:42:43 EST 2007</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>
```

## 3. View the password. Use the ID provided by the output of the previous command.

```
capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword TargetAccount.ID=1
reason=Power Outage reasonDetail=Recovery
```

## 4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.warningMessage>You have this account checked out.</cr.warningMessage>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<ID>1</ID>
<privileged>false</privileged>
<aliases/>
<password>cspmpw</password>
<targetApplicationID>1</targetApplicationID>
<passwordViewPolicyID>6</passwordViewPolicyID>
<cacheBehavior>useCacheFirst</cacheBehavior>
<cacheAllow>true</cacheAllow>
<targetServerAlias/>
```

```

<accessType/>
<userName>cspmuser</userName>
<cacheDuration>30</cacheDuration>
<synchronize>>false</synchronize>
<lastVerified>Wed Sep 10 14:31:08 UTC 2008</lastVerified>
<passwordVerified>>false</passwordVerified>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<createDate>Wed Sep 10 15:31:08 UTC 2008</createDate>
<createUser>admin</createUser>
<hash>GiyMJ8e6bKzDrQgkbp/tPRZPXQ=</hash>
<updateDate>Wed Sep 10 15:31:08 UTC 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType>windows</extensionType>
</TargetAccount>
</cr.result>
</CommandResult>

```

### **Check In an Account Password Using the CLI**

Use the following procedure to check in an account password using the `checkInAccountPassword` command.

#### **Follow these steps:**

1. Search target accounts to retrieve the target account ID of the account that was previously checked out:

```

capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount
TargetAccount.userName=account1

```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **1**.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 UTC 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 UTC 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>14adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>>true</cacheAllow>
<cacheDuration>20</cacheDuration>
<privileged>>false</privileged>
<synchronize>>false</synchronize>
<passwordVerified>>false</passwordVerified>
<lastVerified>Mon Nov 12 15:42:43 EST 2007</lastVerified>
</TargetAccount>

```

```
</cr.result>
</CommandResult>
```

3. Check in the password. Use the ID provided by the output of the previous command.

```
capam_command adminUserID=admin capam=mycompany.com cmdName=checkInAccountPassword TargetAccount.ID=1
```

4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewRequest>
<status>1</status>
<targetAccountID>1</targetAccountID>
<startDate>Wed Sep 10 15:34:00 UTC 2008</startDate>
<endDate>Wed Sep 10 19:34:00 UTC 2008</endDate>
<requestorID>1</requestorID>
<approverID>-1</approverID>
<ID>3</ID>
<createDate>Wed Sep 10 14:34:51 UTC 2008</createDate>
<createUser>admin</createUser>
<hash>fcWQRQVNDogOFxpvm/DLZGlu614=</hash>
<updateDate>Wed Sep 10 15:34:51 UTC 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType/>
</PasswordViewRequest>
</cr.result>
</CommandResult>
```

### **Force an Account Check-In Using the CLI**

When you check out an account, this action restricts others from viewing the password and from changing the account. However, sometimes the administrator must override this restriction. If an administrator wants to access a checked-out account, the administrator can force a check-in of the account on behalf of another user. When the administrator forces a check-in, any required activities for that operation also occur, for example, an update of the account password.

**Follow these steps:**

1. Search target accounts to retrieve the target account ID of the account that was previously checked out:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount
TargetAccount.userName=account1
```

2. Enter your password at the prompt.

Credential Manager returns the following XML command string. Note the ID value. In this example, it is **1**.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
```

```

<createDate>Mon Nov 12 15:42:43 UTC 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 UTC 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>14adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>Mon Nov 12 15:42:43 EST 2007</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>

```

3. Check in the password. Use the ID provided by the output of the previous command.

```
capam_command adminUserID=admin capam=mycompany.com cmdName=forceCheckInAccountPassword TargetAccount.ID=1
```

4. Enter your password at the prompt.

Credential Manager returns the following XML command string.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<PasswordViewRequest>
<status>1</status>
<targetAccountID>1</targetAccountID>
<startDate>Wed Sep 10 15:34:00 UTC 2008</startDate>
<endDate>Wed Sep 10 19:34:00 UTC 2008</endDate>
<requestorID>1</requestorID>
<approverID>-1</approverID>
<ID>3</ID>
<createDate>Wed Sep 10 14:34:51 UTC 2008</createDate>
<createUser>admin</createUser>
<hash>fcWQRQVNDogOFxpvm/DLZGlu614=</hash>
<updateDate>Wed Sep 10 15:34:51 UTC 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType/>
</PasswordViewRequest>
</cr.result>
</CommandResult>

```

## Enable Email Notifications for Viewed Passwords

The *email notification* option for a password view policy allows certain users to receive email notifications when another user views an account password. Emails are sent only for successful initial password view requests. For example, if the password is viewed for an already checked out account, no email is sent.



When adding or updating the policy, select a new set of users to receive email notification or select dual authorization approvers. You can also send the email notification only to the active users from the list of identified users.

#### NOTE

Dual authorization is not required for email notifications.

Enable email notifications in the password view policy.

#### Follow these steps:

1. Select **Credentials, Workflow, Password View Policies**. The Password View Policies page appears.
2. Select the password view policy for which Email Notification is to be enabled and select the **Update** button. The Update Password View Policy dialog appears.
3. Select the **Email Notification** tab and set the **Email Notification** option.
4. Optionally, to send emails to only active users, select **Active Users Only**. Active users can be dual authorization approvers or a new set of users.
5. Optionally, if dual authorization is enabled for this policy, and you want only approvers to receive emails, select **Dual Authorization Approvers Only**. Assign the users by moving them from the **Available Users** list to the **Selected Users** list.

#### WARNING

To receive email notifications, the selected users must have an account with the **Password Manager** role assigned. The email address that is associated with the user account is used.

6. Select **OK**.

#### Configure the Email Settings

The email server and email messages are configured in the Credential Manager email settings. Access these settings by selecting **Settings, Credential Manager**. For instructions on the email settings, see [Configure the Email Server and Email Templates](#).

### Track Account Movement Across Active Directory OUs

Credential Manager can track user accounts that move between different organizational units (OUs) in Active Directory.

When an account changes OUs, the account DN changes. Credential Manager account tracking can find the user account in Active Directory and successfully change the password. Password view policies and password rollover are not impacted by the change to an OU.

Credential Manager first tries to bind to Active Directory using the Distinguished Name (DN). If that binding fails, it tries to bind using the User Principal Name (UPN). If the UPN binding works, the DN is updated in the PAM database to match the DN in Active Directory.

#### Accounts that Do Not Use the UPN

Credential Manager might not be able to track the account change automatically under the following circumstances. Manual updates are required.

- If the Active Directory account does not include a UPN, manually update the DN in the target account. Without a UPN, there is no alternative to the DN.
- If the UPN changes in the Active Directory account, manually update the UPN in the PAM target account. The UPN between Active Directory and Credential Manager must be in sync. Credential Manager can still track an account using the DN. However, any subsequent OU change can alter the DN and the UPN is needed as an alternative.

#### NOTE

Changes only to the UPN do not change the DN.

## See a List of Password View Requests

You can see a list of all password view requests, provided you have the requisite permission. You can also see a list of only your own requests. Both options are available from the **Credentials**, **Workflow** menu. Follow these steps:

1. Go to **Credentials**, **Workflow**, **My Requests**, or **All Requests**.
2. The All Password View Requests or My Password View Requests page display.  
Both pages list the same columns, but the **All Requests** page has a **Delete** button to remove entries.
3. Select **View** to see details of a particular request.

## Make a Request to View a Password

With password view policies established, users and administrators with the required privileges can view passwords. Credential Manager administrators must have appropriate permissions to view passwords and password histories.

### Make a View Password Request Using the UI

Follow these steps:

1. Navigate to **Credentials**, **Manage Targets**, **Accounts**.
2. Do *one* of the following tasks.
  - **From the Target Accounts page:** Select the icon that resembles an eye in the **Action** column of the Account whose password you want to see. A Show Credential pop-up window appears, displaying the account name and credential.
  - **From the account Update page:** Select the name of the account and select the **Update** button. In the Update dialog that appears, select the icon that resembles an eye to the right of the **Credential** field.  
For compound accounts, a drop-down list of all target servers appears in a pop-up window. Select the target server whose password you want to view. Typically, the password is the same for all servers. However, if a password update fails, each server on which the subsequent rollback fails has an out-of-sync password.
3. Select the viewing interval. Times are given based on your local time zone, as set in the Preferences page.
4. Enter your password in the **Password** field.
5. Select the **Reason** for viewing the password from the drop-down list.  
Depending on your organizational policy, your reason can also require a **Reason Description** or a **Reason Code**.

#### **TIP**

Using the CLI, you can customize the list of reasons for viewing a password. See [Customize the Reasons for Viewing a Password](#).

The reference code is shown only if the requestor enters the reference code in the View Account Password Request screen before requesting password authorization.

6. Select **View**.

### View an Account Password from the Access Page

Active Target Applications and their associated Target Accounts are listed on the Access page. Every Target Application that is associated with a Device is identified in the drop-down list in the Target Applications column. Every Target Account that is associated with each application appears in a nested list.

After selecting a target account from the drop-down list, a pop-up window appears with a View Account Password Request window. After entering the password (for the currently logged-in user), the credentials are displayed.

## **View Password History from the UI**

### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**. The Target Accounts page appears with a list of existing accounts.
2. In the account list, select the account for which you want to view the password history. The Account Details page appears.
3. On the **Credential** tab, select the View History icon (a clock with a clockwise arrow) located to the right of the Credential field. The Password History page appears showing password change history.  
The Password History Compromised flag may be manually set within Credential Manager. The flag may be used to record whether a password has become known to an unauthorized individual. The flag may be set to true to indicate that a password should not be reused. The value of the flag does not affect Credential Manager processing.

## **Set Password History Compromised Flag from the UI**

### **Follow these steps:**

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the account with the compromised password.
3. Select the **View History** icon located to the right of the **Credential** field. The **View History** icon resembles a clock with a clockwise arrow.
4. Select the date and time of the credential request. The Password History details page appears.
5. Select the **Compromised** check box.
6. Select **Save**.

## **View Target Passwords from the CLI**

### **Follow these steps:**

1. Search target accounts to retrieve the target account ID:  

```
capam_command adminUserID=admin capam=mycompany.com cmdName=searchTargetAccount
TargetAccount.userName=account1
```
2. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 EST 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>14adc6a1a720e58ee52032364b98f95b</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheDuration>20</cacheDuration>
```

```

<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>Mon Nov 12 15:42:43 EST 2007</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>

```

3. Request to view the password. Use the ID provided by the output of the previous command:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=viewAccountPassword TargetAccount.ID=1
reason=Power Outage reasonDetail=Recovery
```

For compound accounts, you can specify the `TargetServer.hostName` parameter to view the password for a specific server. This parameter is only required for compound server accounts.

4. Enter your password at the prompt. Credential Manager returns the following XML command string.

```

<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<TargetAccount>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.changePasswordAfterViewing>true</Attribute.changePasswordAfterViewing>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:42:43 EST 2007</createDate>
<updateDate>Mon Nov 12 15:42:43 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>q3/BaUy9uPvtbUkKgIrXvgseGt8=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>account1</userName>
<password>123456</password>
<accessType>A</accessType>
<cacheAllow>true</cacheAllow>
<cacheDuration>20</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>2007-11-12 15:42:43.0</lastVerified>
</TargetAccount>
</cr.result>
</CommandResult>

```

## Configure Just in Time (JIT) Provisioning for MSSQL User Accounts

This section describes how to configure Just in Time (JIT) provisioning to dynamically provision and deprovision Microsoft SQL Server (MSSQL) user accounts on demand.

JIT provisioning provides the following security enhancements for access to your SQL Server database:

- Zero-trust security where user identities only exist on SQL Server during the checkout period.
- On-demand identity and access management with dynamic privileges that is auditable and can be subject to third-party approval.

Key components introduced to support JIT dynamic provisioning are:

- *Custom workflows* that are used to define custom directives to execute when a PAM user checks out and checks in target account credentials
- *Provisioned accounts* that are used as a template for dynamically creating target accounts. These target accounts are provisioned when credentials are checked out and deleted when they are checked in.

### Prerequisites

- An Active Directory domain server that is configured as an LDAP directory in PAM and containing the users and user groups to be imported into PAM.
- A supported Microsoft SQL Server database on a server that is a member of the previously described LDAP domain.

### Configuration Steps

To configure JIT provisioning, complete the following procedures in order:

1. [Add the LDAP Domain Server Required for JIT Provisioning](#)
2. [Import LDAP User Groups for JIT Provisioning](#)
3. [Create a Device for the MSSQL Database That Requires JIT Provisioning](#)
4. [Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in](#)
5. [Create a Target Application for the MSSQL Database Admin Account Used by JIT Provisioning](#)
6. [Create a Target Account for the MSSQL Database Administrator \(for JIT Provisioning\)](#)
7. [Configure a Provisioned Account for JIT Provisioning](#)
8. [\(Optional\) Restrict Users from Editing Azure User Name Values](#)
9. [Create an Access Policy for JIT LDAP Users](#)

## Add the LDAP Domain Server Required for JIT Provisioning

This procedure describes how to configure PAM to communicate with an LDAP domain server that contains the users and groups that require JIT provisioning.

### Follow these steps:

1. Do the following steps to create a target device for the LDAP domain server:
  - a. Navigate to **Devices, Manage Devices**
  - b. Select the **Add** button.
  - c. Complete the following fields in the **Add Device** pane that opens:
    - **Name**: A descriptive name for the device.
    - **Address**: The IP address of the LDAP domain server.
    - **Device type**: Set the **Access** and **Password Management** options.
2. Do the following steps to configure a target application for the domain server:
  - a. Navigate to **Credentials, Manage Targets, Applications**.
  - b. Select the **Add** button.
  - c. Complete the following fields on the **Application** tab of the **Add Target Application** pane that opens:
    - **Host Name**: The IP address or FQDN of the LDAP domain server.
    - **Device Name**: The name of the domain server.
    - **Application Name**: The name of the target application.
    - **Application Type**: Select **Active Directory** from the drop-down menu.
  - d. Select the **Active Directory** tab and enter the desired domain name (for example, examplead.com).
3. Do the following steps to configure a target account for the domain administrator:
  - a. Navigate to **Credentials, Manage Targets, Accounts**.
  - b. Select the **Add** button.
  - c. Complete the following fields on the **Account** tab of the **Add Target Account** pane that opens:

- **Host Name:** The IP address or FQDN of the LDAP domain server.
  - **Device Name:** The name of the domain server.
  - **Application Name:** The name of the domain server target application.
  - **Account Name:** The name of the domain administrator account.
  - **Password View Policy:** The required password view policy.
  - **Password:** Specify the password of the domain administrator account.
- d. Select the **Active Directory** tab and enter the DN of the domain administrator account in the **Distinguished Name** field. For example: CN=Administrator,CN=Users,DC=EXAMPLEAD,DC=com
4. Do the following steps to configure the LDAP domain for the LDAP server:
- a. Navigate to **Configuration, 3rd Party, LDAP**.
  - b. Select the **Add** button.
  - c. Complete the following fields on **Add LDAP Domain** pane that opens:
    - **Bind Server:** The IP address of the LDAP domain target server.
    - **Bind Application:** The domain server target application.
    - **Bind Account:** The domain administrator target account.
    - **Server:** Select the plus icon and specify the IP address and port number of the LDAP domain.

**TIP**

**Next step:** [Import LDAP User Groups for Azure SQL JIT Provisioning](#).

## Import LDAP User Groups for JIT Provisioning

This topic describes how to import LDAP user groups that contain the MSSQL users and groups that require JIT provisioning.

### Follow these steps:

1. Connect to PAM using the PAM client.
2. Navigate to **Users, Manage User Groups, Import LDAP Groups**. The LDAP Browser opens.
3. Select **File, Connect**.
4. In the **Connect to LDAP Domain** dialog that opens, select the LDAP domain that you configured to communicate with your LDAP domain server and select **OK**.
5. Locate and expand the **Users** folder from the LDAP tree in the left pane.
6. Locate and select the checkbox beside each user group that you want to import.
7. (Optional) Review the device groups that are selected for import:
  - a. Select **PAM Groups, Manage selected groups to register with the PAM appliance**.  
The list of the Distinguished Names for all selected groups displays.
  - b. Select and edit any group DN, or remove it from the staging list.
8. Select **PAM Groups, Register selected groups with the PAM appliance**. A window opens displaying a list of the staged groups from which you can monitor progress, and can display any messages that are associated with the actions.
 

**Note:** When you import a group, all the users that are members of that group are imported into PAM automatically.
9. Select **Register Groups** in the lower-left corner. PAM imports the groups in the order that they are listed. The browser provides feedback and cancellation options throughout the process
10. When the import is complete and verified, close the LDAP browser.
11. In the PAM UI, navigate to **Users, Manage User Groups**, and confirm that the imported user groups appear.
12. Navigate to **Users, Manage Users**, and confirm that the users in the imported user groups appear on the page.
13. Update the definition of each imported user to define an **RDP User Name** that specifies the LDAP domain name and the user name specified in the user information using the following format: *LDAP\_Domain\SAM\_Account\_Name*  
For example: JITDOMAIN\joe

**Note:** If you have imported a large number of users, we recommend that you use the External API to automate the RDP User Name update for those users.

14. Assign appropriate PAM roles to each user and group based on your organizational requirements.

**TIP**

**Next step:** [Create a Device for the MSSQL Database That Requires JIT Provisioning.](#)

## Create a Device for the MSSQL Database That Requires JIT Provisioning

This topic describes how to create a device for the Microsoft SQL Server (MSSQL) database on which you require Just in Time dynamic provisioning and deprovisioning of user accounts

**Follow these steps:**

1. Navigate to **Devices, Manage Devices**
2. Select the **Add** button.
3. Complete the following fields in the **Add Device** pane that opens:
  - **Name:** A descriptive name for the device (Provisioned Account, “SQL 2019”).
  - **Address:** The IP address of the SQL Server.
  - **Device type:** Set the **Access** and **Password Management** options.

**TIP**

**Next step:** [Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in .](#)

## Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in

Configure a Custom Workflow that defines the directives to execute when a PAM user checks out and checks in a target account using Just in Time (JIT) provisioning on an MSSQL or Azure SQL managed instance.

### Credential Manager Privileges Required to Work with Custom Workflows

Administrators responsible for creating, updating, and deleting custom workflows must be assigned a role with the following Credential Manager privileges (as appropriate):

- **Add Custom Workflow:** Required to create a new custom workflow.
- **Delete Custom Workflow:** Required to delete a custom workflow.
- **Update Custom Workflow:** Required to update a custom workflow.
- **Read Custom Workflow:** Required to view a custom workflow.
- **Search Custom Workflow:** Required to search for and list custom workflows.

For a complete list of Credential Manager roles and privileges, see [Add or Modify Credential Manager Roles.](#)

### Directives for MSSQL JIT Custom Workflows

Use the following directives when configuring actions to run on the target database when a user checks out or checks in a target account:

**Note:** Use the exact syntax used in the following samples.

Application Type	Required Operation	Directive
MSSQL	Create account	+Account
MSSQL	Remove account	-Account
MSSQL	Add a role	+Role:<role name>



MSSQL	Remove a role	-Role:<role name>
MSSQL	Add multiple roles	+Role:<role1 name>,<role2 name>
MSSQL	Remove multiple roles	-Role:<role1 name>,<role2 name>
MSSQL	Create Account and update roles	+Account;+Role:<role1 name>,<role2 name>

### Directives for Azure SQL Managed Instance JIT Custom Workflows

Use the following directives when configuring actions to run on the target database when a user checks out or checks in a target account:

**Note:** Use the *exact* syntax used in the following samples.

Application Type	Required Operation	Directive
MSSQL Azure Managed Instance	Create account	+Account
MSSQL Azure Managed Instance	Remove account	-Account
MSSQL Azure Managed Instance	Add a role	+Role:<role name>
MSSQL Azure Managed Instance	Remove a role	-Role:<role name>
MSSQL Azure Managed Instance	Add multiple roles	+Role:<role1 name>,<role2 name>
MSSQL Azure Managed Instance	Remove multiple roles	-Role:<role1 name>,<role2 name>
MSSQL Azure Managed Instance	Create Account and update roles	+Account;+Role:<role1 name>,<role2 name>

### Create and Configure a Custom Workflow

Follow this procedure to create and configure a custom workflow

**Follow these steps:**

1. Navigate to **Credentials, Workflow, Custom Workflows**.
2. In the **Custom Workflows** panel that opens, select the **Add** button to create a new custom workflow. The **Add Custom Workflow** pane opens.
3. Provide the high-level details of the custom workflow:
  - **Name:** The name of the custom workflow.
  - **Description:** Optionally, add some high level details about the directives that the workflow executes on check and check-in operations. Provisioned Account, "Create an account with roles on checkout; remove account on check-in."
  - **Application Type:** Select the appropriate application type: **MSSQL** or **MSSQL Azure Managed Instance**.
4. Do the following steps to create a custom workflow action for check-out operations:
  - a. Select the **Add** button. The **Add Custom Workflow Action** dialog opens.
  - b. Select **Check-Out** from the **Action** drop-down menu  
Enter an appropriate directive in the **Commands** field. Provisioned Account, to create a database login account with roles *dbcreator* and *diskadmin* on checkout enter the following directive: +Account;+Role:dbcreator,diskadmin
  - c. Select the **OK** button. You are returned to the **Add Custom Workflow** pane.



5. Do the following steps to create a custom workflow action for check-in operations:
  - a. Select the **Add** button. The **Add Custom Workflow Action** dialog opens.
  - b. Select **Check-In** from the **Action** drop-down menu
 Enter the –Account directive in the **Commands** field.  
 Select the **OK** button. You are returned to the **Add Custom Workflow** panel.
6. Select **OK** to submit the custom workflow.

**TIP**

**Next step:** One of the following, as appropriate:

- [Create a Target Application for the MSSQL Database Admin Account Used by JIT Provisioning](#)
- [Provide an Administrator Account to Use to Access the Azure SQL Managed Instance for JIT Provisioning](#)

## Create a Target Application for the MSSQL Database Admin Account Used by JIT Provisioning

This topic describes how to create a target application for the Microsoft SQL Server (MSSQL) database account required to implement Just in Time dynamic provisioning and deprovisioning of user accounts.

**Follow these steps:**

1. Navigate to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Target Application** pane that opens:
  - **Host Name:** Specify the device that you created for the SQL Server.
  - **Application Name:** Specify a name for the application.
  - **Application Type:** Select **MSSQL** from the drop-down menu.

**TIP**

**Next step:** [Create a Target Account for the MSSQL Database Administrator \(for JIT Provisioning\)](#).

## Create a Target Account for the MSSQL Database Administrator (for JIT Provisioning)

This topic describes how to create a target account for the MSSQL database administrator, which is used to access the MSSQL database.

**Follow these steps:**

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Target Account** pane that opens:
  - **Host Name:** The IP address or FQDN of the MSSQL Server.
  - **Device Name:** The name of the MSSQL Server.
  - **Application Name:** The name of the MSSQL Server target application.
  - **Account Name:** The name of the MSSQL server administrator account, for example "sa".
  - **Password View Policy:** The name of the required password view policy, for example "default".
  - **Password:** Specify the password of the MSSQL Server administrator account.

**TIP**

**Next step:** [Configure a Provisioned Account for JIT Provisioning](#).

## Configure a Provisioned Account for JIT Provisioning

A *provisioned account* is a special target account used as a template for dynamic provisioning. The provisioned account is saved as a reference point but resolves as the personal account of the user. To comply with zero trust, the personal account does not exist in PAM or at the target server until it is required by the user.

Any action taken is based upon the directives configured in the associated custom workflow.

### NOTE

PAM currently supports checkout and check-in custom workflow operations.

Do the following procedures to configure a provisioned account for JIT Provisioning:

1. [Create a Password View Policy for the JIT Provisioned Account](#)
2. [Create a Target Application for the JIT Provisioned Account](#)
3. [Create a Target Account for the MSSQL JIT Provisioned Account](#)

## Create a Password View Policy for the JIT Provisioned Account

This topic describes how to configure a password view policy for the JIT provisioned account, which is used as a template for dynamic provisioning.

Follow these steps:

1. Navigate to **Credentials, Workflow, Password View Policies**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Password View Policy** pane that opens:
  - **Name:** Specify a descriptive name for the password view policy.
  - **Description:** Optionally, provide a description for the password view policy.
  - **Check-Out/Check-In:** Set this option to enable the custom workflow that you configured to execute when a PAM user checks out and checks in a target account.
4. Optionally, configure other compatible options (see the following note) to comply with organizational requirements.

### IMPORTANT

Do not set any of the following options, which are incompatible with JIT provisioning:

- **Change Password on view**
- **Change Password On Connection End**
- **Re-authenticate For Auto Connect**
- **Reason Required For Auto Connect**
- **Change Password On Auto Connect**
- **Change Password On Session End**

### TIP

**Next step:** [Create a Target Application for the JIT Provisioned Account](#).

## Create a Target Application for the JIT Provisioned Account

This topic describes how to create a target application for the JIT Provisioned Account, which is used for dynamically creating user accounts.

Follow these steps:

1. Navigate to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Target Application** pane that opens:

- **Host Name:** Specify the device that you created for the SQL Server.
- **Application Name:** Specify a name for the application.
- **Application Type:** Select **MSSQL** from the drop-down menu.
- **Custom Workflow:** Select the Custom Workflow that you created earlier.

**TIP**

**Next step:** [Create a Target Account for the MSSQL JIT Provisioned Account.](#)


## Create a Target Account for the MSSQL JIT Provisioned Account


This topic describes how to configure a target account for the JIT Provisioned Account, which is used for dynamically creating user accounts.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.
3. Complete the following fields on the **Account** tab on the **Add Target Account** pane that opens:
  - a. **Host Name:** The IP address or FQDN of the SQL Server.
  - b. **Device Name:** The name of the SQL Server.
  - c. **Provisioned Account:** (Located at the bottom of the listed options.) Set this option to configure this target account as a template for dynamically creating user accounts to support JIT provisioning.

**NOTE**

Setting the **Provisioned Account** option activates a search icon (  ) beside the **Account Name** field that is required to select an identity template.

- d. **Application Name:** The name of the MSSQL Server target application that you created for the provisioned account.
- e. **Password View Policy:** The name of the password view policy that you created for the provisioned account.
- f. **Account Name:** To specify the account name, follow these steps:
  - a. Select the search (  ) icon.
 

**NOTE**

If the search icon is not present, verify that the **Provisioned Account** option (located at the bottom of the listed options) is set.
  - b. Select the **RDP User Name** entry from the **Extended Identity Templates** dialog that opens.
  - c. Select **OK**.  
The **Account Name** field is populated with the value from the **Template** column on the **Extended Entity Templates** dialog ( `${User.rdpUsername}` ).
  - g. **Password:** Any text that matches the password composition policy for the target application (provisioned account passwords are not managed within PAM).
4. On the **MSSQL** tab, set the **Use the following account to administer changes** option, and use one of the following options to identify the target account that you created when configuring the connection to Azure:

- Enter the name of the target account in the text box.
- Select the **Search** icon (🔍) and choose the appropriate account from the **Target Accounts** dialog that appears, as shown in the following example

### Target Accounts

Column: Application Type Value: MSSQL 🔍 ↺

Account Name	Application Name	Application	Host Name	Device Name	Account Type	Owner User	Verified
\${User.userPrincipalName}	MSSQL JIT	MSSQL	10.252.5...	MSSQL	Privileged		
sa	MSSQL DB	MSSQL	10.252.5...	MSSQL	Privileged		✓

screenshot:

#### NOTE

When a user performs checkout and check-in operations using a provisioned account, their account name is replaced with the RDP User Name set in the User Information (Provisioned Account, *MYLDAP\TestUser1*) on the **Access** page.

#### TIP

**Next step:** [Create a Password View Policy for the JIT Provisioned Account.](#)

## (Optional) Restrict Users from Editing RDP User Name Values

Most users inherit the "Manage User RDP User Name" privilege that is required to edit the **RDP User Name** in user definitions from their assigned role.

The following roles provide the "Manage User the RDP Username" privilege:

- Standard user
- User/Group Manager
- Delegated Administrator
- Operational Administrator
- Global Administrator
- Server Control Administrator
- UNAB Manager

For a complete list of user roles and privileges, see [User Roles](#).

**To prevent users from editing the "RDP User name" field:** Create a custom role with user privileges that do not include or inherit the "Manage User RDP User Name" privilege. For more information, see [Add or Modify Credential Manager Roles](#).

#### TIP

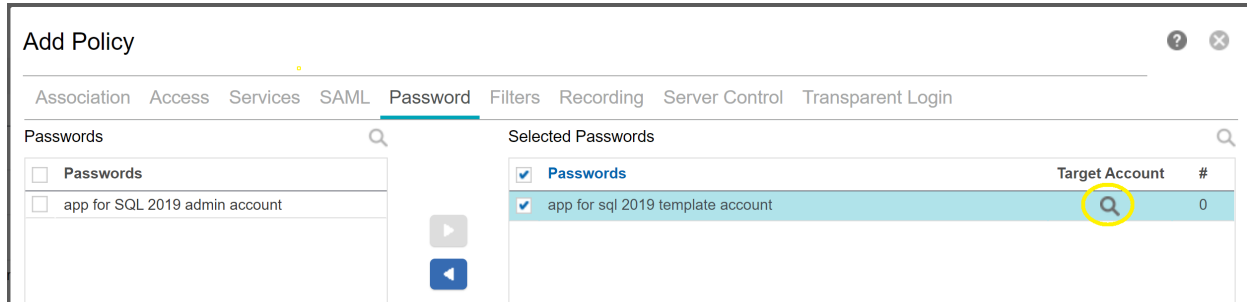
**Next step:** [Create an Access Policy for JIT LDAP Users.](#)

## Create an Access Policy for JIT LDAP Users

Create an access policy that defines the device that users imported from the LDAP domain server for Just in Time provisioning can access and the properties of that relationship.

1. Navigate to **Policies, Manage Policies**.
2. Select the **Add** button.

3. Complete the following fields on the **Association** tab of the **Add Policy** pane that opens:
  - **User or User Group:** Complete *one* of these fields with the Distinguished Name (DN) of the required user or group.  
**Tip:** Use the Search icon to display the list of choices, select the required user or group from the drop-down list, and then select **OK**.
  - **Device or Device Group Name:** Complete the **Device** field with the name of the device for which the policy controls access.
4. Do the following steps on the **Password** tab:
  - a. Select the target application that you created for the provisioned account in the **Passwords** column and move it to the **Selected Passwords** column.
  - b. Select the magnifying glass icon in the **Target Account** column (highlighted in the following screen capture):



- c. Select the target account that you created for the provisioned account and move it to the **Selected Target Account** column.
- d. Select **OK**.

## User Experience: Just in Time (JIT) Checkout and Check-in Operations

This section describes how a user from the LDAP domain server and configured in the JIT access policy checks out and checks in credentials.

1. Launch the PAM client, connect to PAM, and do the following steps to log in:
  - a. Enter your username and password in the corresponding fields.
  - b. Select **LDAP** from the **Authentication Type** drop-down menu
  - c. Select the name of the LDAP domain configured for JIT from the **Domain** drop-down menu.
2. To check out credentials for a device, do the following steps on the **Access** page:
  - a. Click the **Select** icon in the **Target Applications** column of the device entry. The name of the target application and your RDP account name appear.
  - b. Select the account name. A **Custom Workflow Checkout Status** pane opens, showing execution details, including messages related to the directives executed along with the status of the checkout operation.
3. To check in the credentials, return to the **Access** page and select the corresponding **Check-in** link available under the **Passwords currently in use** heading. A **Custom Workflow Check-in Status** pane opens showing execution details, including messages related to the directives executed and the status of the check-in operation.

## Configure Just in Time (JIT) Provisioning for Azure SQL Managed Instance User Accounts

This section describes how to configure Just in Time (JIT) provisioning to dynamically provision and deprovision Azure SQL Managed Instance user accounts on demand.

JIT provisioning provides the following security enhancements for access to your Azure SQL Managed Instance:

- Zero-trust security where user identities only exist on Azure SQL Managed Instance during the checkout period.
- On-demand identity and access management with dynamic privileges that is auditable and can be subject to third-party approval.

Key components introduced to support JIT dynamic provisioning are:

- Custom workflows that are used to define custom directives to execute when a PAM user checks out and checks in target account credentials
- Provisioned accounts that are used as a template for dynamically creating target accounts. These target accounts are provisioned when credentials are checked out and deleted when they are checked in.

### Prerequisites

- A supported Azure SQL Managed Instance (MI) Database on Azure.
- An Active Directory domain server.

### Configuration Steps

To configure JIT provisioning, complete the following procedures in order:

1. [Add the LDAP Domain Server Required for JIT Provisioning](#)
2. [Import LDAP User Groups for Azure SQL JIT Provisioning](#)
3. [Create a Device for the Azure SQL Managed Instance That Requires JIT Provisioning](#)
4. [Create a Custom Workflow to Handle Azure SQL Managed Instance JIT Target Account Checkout and Check-in](#)
5. [Provide an Administrator Account to Use to Access the Azure SQL Managed Instance for JIT Provisioning](#)
6. [Configure a Provisioned Account for Azure SQL Managed Instance JIT Provisioning](#)
7. [\(Optional\) Restrict Users from Editing Azure User Name Values](#)
8. [Create an Access Policy for Azure Managed Instance JIT LDAP Users](#)

## Add the LDAP Domain Server Required for JIT Provisioning

This procedure describes how to configure PAM to communicate with an LDAP domain server that contains the users and groups that require JIT provisioning.

### Follow these steps:

1. Do the following steps to create a target device for the LDAP domain server:
  - a. Navigate to **Devices, Manage Devices**
  - b. Select the **Add** button.
  - c. Complete the following fields in the **Add Device** pane that opens:
    - **Name:** A descriptive name for the device.
    - **Address:** The IP address of the LDAP domain server.
    - **Device type:** Set the **Access** and **Password Management** options.
2. Do the following steps to configure a target application for the domain server:
  - a. Navigate to **Credentials, Manage Targets, Applications**.
  - b. Select the **Add** button.
  - c. Complete the following fields on the **Application** tab of the **Add Target Application** pane that opens:
    - **Host Name:** The IP address or FQDN of the LDAP domain server.
    - **Device Name:** The name of the domain server.
    - **Application Name:** The name of the target application.
    - **Application Type:** Select **Active Directory** from the drop-down menu.
  - d. Select the **Active Directory** tab and enter the desired domain name (for example, examplead.com).
3. Do the following steps to configure a target account for the domain administrator:
  - a. Navigate to **Credentials, Manage Targets, Accounts**.

- b. Select the **Add** button.
  - c. Complete the following fields on the **Account** tab of the **Add Target Account** pane that opens:
    - **Host Name:** The IP address or FQDN of the LDAP domain server.
    - **Device Name:** The name of the domain server.
    - **Application Name:** The name of the domain server target application.
    - **Account Name:** The name of the domain administrator account.
    - **Password View Policy:** The required password view policy.
    - **Password:** Specify the password of the domain administrator account.
  - d. Select the **Active Directory** tab and enter the DN of the domain administrator account in the **Distinguished Name** field. For example: CN=Administrator,CN=Users,DC=EXAMPLEAD,DC=com
4. Do the following steps to configure the LDAP domain for the LDAP server:
- a. Navigate to **Configuration, 3rd Party, LDAP**.
  - b. Select the **Add** button.
  - c. Complete the following fields on **Add LDAP Domain** pane that opens:
    - **Bind Server:** The IP address of the LDAP domain target server.
    - **Bind Application:** The domain server target application.
    - **Bind Account:** The domain administrator target account.
    - **Server:** Select the plus icon and specify the IP address and port number of the LDAP domain.

**TIP**

**Next step:** [Import LDAP User Groups for Azure SQL JIT Provisioning](#).

## Import LDAP User Groups for Azure SQL JIT Provisioning

To allow users to use the same password to log into PAM and the Azure SQL Managed Instance (recommended), import LDAP Azure SQL Managed Instance users and groups into PAM.

### Follow these steps:

1. Connect to PAM using the PAM client.
2. Navigate to **Users, Manage User Groups, Import LDAP Groups**. The LDAP Browser opens.
3. Select **File, Connect**.
4. In the **Connect to LDAP Domain** dialog that opens, select the LDAP domain that you configured to communicate with your LDAP domain server and select **OK**.
5. Locate and expand the **Users** folder from the LDAP tree in the left pane.
6. Locate and select the checkbox beside each user group that you want to import.
7. (Optional) Review the device groups that are selected for import:
  - Select **PAM Groups, Manage selected groups to register with the PAM appliance**. The list of the Distinguished Names for all selected groups displays.
  - Select and edit any group DN, or remove it from the staging list.
8. Select **PAM Groups, Register selected groups with the PAM appliance**. A window opens displaying a list of the staged groups from which you can monitor progress, and can display any messages that are associated with the actions. **Note:** When you import a group, all the users that are members of that group are imported into PAM automatically.
9. Select **Register Groups** in the lower-left corner. PAM imports the groups in the order that they are listed. The browser provides feedback and cancellation options throughout the process
10. When the import is complete and verified, close the LDAP browser.
11. In the PAM UI, navigate to **Users, Manage User Groups**, and confirm that the imported user groups appear.
12. Navigate to **Users, Manage Users**, and confirm that the users in the imported user groups appear on the page.
13. For *each* imported user, do one of the following operations on the **Extended Identities** tab:



- (Optional) If the user principal name assigned to the user in LDAP (and imported into PAM) is the required username for the account, verify that the entry in the **Value** field in the **User Principal Name** row is correct.
- If the user principal name assigned to the user in LDAP is not specified or is not the correct username, enter the appropriate username in the **Value** field in the **Azure Username** row.

**NOTE**

If you have imported a large number of users, we recommend that you use the External API to automate the Azure username update for those users.

14. Assign appropriate PAM roles to each user and group based on your organizational requirements.

**TIP**

**Next step:** [Create a Device for the Azure SQL Managed Instance That Requires JIT Provisioning.](#)

## Create a Device for the Azure SQL Managed Instance That Requires JIT Provisioning

This topic describes how to create a device for the Azure SQL Managed Instance on which you require Just in Time dynamic provisioning and de-provisioning of user accounts

**Follow these steps:**

1. Navigate to **Devices, Manage Devices**
2. Select the **Add** button.
3. Complete the following fields in the **Add Device** pane that opens:
  - **Name:** A descriptive name for the device (For example, "Microsoft Azure Target Server").
  - **Address:** The hostname of the Azure SQL Managed Instance. For example, example-sqlmi-1.3e83051ceee4.database.windows.net.
  - **Device type:** Set the **Password Management** options.

**TIP**

**Next step:** [Create a Custom Workflow to Handle Azure SQL Managed Instance JIT Target Account Checkout and Check-in.](#)

## Create a Custom Workflow to Handle Just in Time Target Account Checkout and Check-in

Configure a Custom Workflow that defines the directives to execute when a PAM user checks out and checks in a target account using Just in Time (JIT) provisioning on an MSSQL or Azure SQL managed instance.

**Credential Manager Privileges Required to Work with Custom Workflows**

Administrators responsible for creating, updating, and deleting custom workflows must be assigned a role with the following Credential Manager privileges (as appropriate):

- **Add Custom Workflow:** Required to create a new custom workflow.
- **Delete Custom Workflow:** Required to delete a custom workflow.
- **Update Custom Workflow:** Required to update a custom workflow.
- **Read Custom Workflow:** Required to view a custom workflow.
- **Search Custom Workflow:** Required to search for and list custom workflows.

For a complete list of Credential Manager roles and privileges, see [Add or Modify Credential Manager Roles.](#)



### Directives for MSSQL JIT Custom Workflows

Use the following directives when configuring actions to run on the target database when a user checks out or checks in a target account:

**Note:** Use the *exact* syntax used in the following samples.

Application Type	Required Operation	Directive
MSSQL	Create account	+Account
MSSQL	Remove account	-Account
MSSQL	Add a role	+Role:<role name>
MSSQL	Remove a role	-Role:<role name>
MSSQL	Add multiple roles	+Role:<role1 name>,<role2 name>
MSSQL	Remove multiple roles	-Role:<role1 name>,<role2 name>
MSSQL	Create Account and update roles	+Account;+Role:<role1 name>,<role2 name>

### Directives for Azure SQL Managed Instance JIT Custom Workflows

Use the following directives when configuring actions to run on the target database when a user checks out or checks in a target account:

**Note:** Use the *exact* syntax used in the following samples.

Application Type	Required Operation	Directive
MSSQL Azure Managed Instance	Create account	+Account
MSSQL Azure Managed Instance	Remove account	-Account
MSSQL Azure Managed Instance	Add a role	+Role:<role name>
MSSQL Azure Managed Instance	Remove a role	-Role:<role name>
MSSQL Azure Managed Instance	Add multiple roles	+Role:<role1 name>,<role2 name>
MSSQL Azure Managed Instance	Remove multiple roles	-Role:<role1 name>,<role2 name>
MSSQL Azure Managed Instance	Create Account and update roles	+Account;+Role:<role1 name>,<role2 name>

### Create and Configure a Custom Workflow

Follow this procedure to create and configure a custom workflow

**Follow these steps:**

1. Navigate to **Credentials, Workflow, Custom Workflows**.
2. In the **Custom Workflows** panel that opens, select the **Add** button to create a new custom workflow. The **Add Custom Workflow** pane opens.
3. Provide the high-level details of the custom workflow:

- **Name:** The name of the custom workflow.
  - **Description:** Optionally, add some high level details about the directives that the workflow executes on check and check-in operations. Provisioned Account, “Create an account with roles on checkout; remove account on check-in.”
  - **Application Type:** Select the appropriate application type: **MSSQL** or **MSSQL Azure Managed Instance**.
4. Do the following steps to create a custom workflow action for check-out operations:
    - a. Select the **Add** button. The **Add Custom Workflow Action** dialog opens.
    - b. Select **Check-Out** from the **Action** drop-down menu  
Enter an appropriate directive in the **Commands** field. Provisioned Account, to create a database login account with roles *dbcreator* and *diskadmin* on checkout enter the following directive: +Account;+Role:dbcreator,diskadmin
    - c. Select the **OK** button. You are returned to the **Add Custom Workflow** pane.
  5. Do the following steps to create a custom workflow action for check-in operations:
    - a. Select the **Add** button. The **Add Custom Workflow Action** dialog opens.
    - b. Select **Check-In** from the **Action** drop-down menu  
Enter the –Account directive in the **Commands** field.  
Select the **OK** button. You are returned to the **Add Custom Workflow** panel.
  6. Select **OK** to submit the custom workflow.

**TIP**

**Next step:** One of the following, as appropriate:

- [Create a Target Application for the MSSQL Database Admin Account Used by JIT Provisioning](#)
- [Provide an Administrator Account to Use to Access the Azure SQL Managed Instance for JIT Provisioning](#)

## Provide an Administrator Account to Use to Access the Azure SQL Managed Instance for JIT Provisioning

The type of administrator account that you require to access the Azure SQL Managed Instance depends on the authentication method that is specified for that instance in Azure:

- **Use only Azure Active Directory (Azure AD) authentication:** If this option is specified, Azure uses the administrator account that is defined for a configured [Azure Active Directory target connection](#). [Proceed to the next step](#).
- **Use both SQL and Azure AD authentication:** If this option is specified, Azure can use either of the following options:
  - The administrator account that is defined for a configured [Azure Active Directory target connection](#).
  - An account that you define in the Azure SQL Managed Instance using the following procedure.
- **Use SQL authentication:** If this option is specified, Azure uses an account that you define in the Azure SQL Managed Instance using the following procedure.

**To define an administrator account in the Azure SQL Managed Instance, follow these steps:**

1. Navigate to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Target Application** pane that opens:
  - **Host Name:** Specify the device that you created for the Azure SQL Managed Instance.
  - **Application Name:** Specify a name for the application.
  - **Application Type:** Select **MSSQL Azure Managed Instance** from the drop-down menu.
4. Navigate to **Credentials, Manage Targets, Accounts**.
5. Select the **Add** button.
6. Complete the following fields on the **Add Target Account** dialog that opens:

- **Host Name:** The FQDN of the Azure SQL Managed Instance. **Tip:** Use the **Search** icon to select the device from the **Target Servers** dialog that opens.
- **Device Name:** The name of the Azure SQL Managed Instance.
- **Application Name:** The name that you specified in the **Application Name** field in Step 3.
- **Account Name:** The name of the Azure SQL Managed Instance administrator account (for example, "sa").
- **Password View Policy:** The name of the required password view policy, for example "default".
- **Password:** Specify the password of the Azure SQL Managed Instance administrator account.

**TIP**

**Next step:** [Configure a Provisioned Account for Azure SQL Managed Instance JIT Provisioning.](#)

## Configure a Provisioned Account for Azure SQL Managed Instance JIT Provisioning

A *provisioned account* is a special target account used as a template for dynamic provisioning. The provisioned account is saved as a reference point but resolves as the personal account of the user. To comply with zero trust, the personal account does not exist in PAM or at the target server until it is required by the user.

Any action taken is based upon the directives configured in the associated custom workflow.

**NOTE**

PAM currently supports checkout and check-in custom workflow operations.

**Do the following procedures to configure a provisioned account for JIT Provisioning::**

1. [Create a Password View Policy for the JIT Provisioned Account](#)
2. [Create a Target Application for the JIT Provisioned Account](#)
3. [Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account](#)

### Create a Password View Policy for the JIT Provisioned Account

This topic describes how to configure a password view policy for the JIT provisioned account, which is used as a template for dynamic provisioning.

**Follow these steps:**

1. Navigate to **Credentials, Workflow, Password View Policies**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Password View Policy** pane that opens:
  - **Name:** Specify a descriptive name for the password view policy.
  - **Description:** Optionally, provide a description for the password view policy.
  - **Check-Out/Check-In:** Set this option to enable the custom workflow that you configured to execute when a PAM user checks out and checks in a target account.
4. Optionally, configure other compatible options (see the following note) to comply with organizational requirements.

**IMPORTANT**

Do not set any of the following options, which are incompatible with JIT provisioning:

- **Change Password on view**
- **Change Password On Connection End**
- **Re-authenticate For Auto Connect**
- **Reason Required For Auto Connect**
- **Change Password On Auto Connect**
- **Change Password On Session End**

**TIP**

**Next step:** [Create a Target Application for the JIT Provisioned Account.](#)

## Create a Target Application for the JIT Provisioned Account

This topic describes how to create a target application for the JIT Provisioned Account, which is used for dynamically creating user accounts.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.
3. Complete the following fields on the **Add Target Application** pane that opens:
  - **Host Name:** Specify the device that you created for the Azure SQL Database.
  - **Application Name:** Specify a name for the application.
  - **Application Type:** Select **MSSQL Azure Managed Instance** from the drop-down menu.
  - **Custom Workflow:** Select the Custom Workflow that you created earlier.

**TIP**

**Next step:** [Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account.](#)

## Create a Target Account for the Azure SQL Managed Instance JIT Provisioned Account

This topic describes how to configure a target account for the Azure SQL Managed Instance JIT Provisioned Account, which is used for dynamically creating user accounts.

### Follow these steps:

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.
3. Complete the following fields in the specified order on the **Account** tab of the **Add Target Account** pane that opens:
  - a. **Host Name:** The IP address or FQDN of the Azure SQL managed instance.
  - b. **Device Name:** The name of the Azure SQL managed instance.
  - c. **Provisioned Account:** (Located at the bottom of the listed options.) Set this option, which is required to configure this target account as a template for dynamically creating user accounts to support JIT provisioning.

**NOTE**

Setting the **Provisioned Account** option activates a search icon (🔍) beside the **Account Name** field that is used to select an identity template.

- d. **Application Name:** The name of the Azure SQL Managed Instance target application that you created for the provisioned account.
- e. **Account Name:** To specify the account name, follow these steps:

- a. Select the search (🔍) icon.

**NOTE**

If the search icon is not present, verify that the **Provisioned Account** option (located at the bottom of the listed options) is set.

- b. Select one of the following **Identity Names** from the **Extended Identity Templates** dialog that opens:
  - **User Principal Name:** Use this option if the user principal name assigned to the user in LDAP (and imported into PAM) was the correct name for the account.
  - **Azure User Name:** Use this option if the user principal name assigned to the user in LDAP is not specified or is not the correct username.
- c. Select **OK**.

The **Account Name** field is populated with the value from the **Template** column from the **Extended Entity Templates** dialog. For example, if you selected **User Principal Name**, the field is populated with the following value: `${User.userPrincipalName}`.

- f. **Password View Policy:** Enter the name of the password view policy that you created for the provisioned account.
  - g. **Password:** Enter a password that conforms to the password composition policy for the target application or select the **Generate Password** icon (🔑) to generate one automatically. (Provisioned account passwords are not managed within PAM.)
4. On the **MSSQL Azure Managed Instance** tab, set the **Use the following account to administer changes** option, and use one of the following options to identify the target account that you created when configuring the connection to Azure:
- Enter the name of the target account in the text box.
  - Select the **Search** icon (🔍) and choose the appropriate account from the **Target Accounts** dialog that appears, as shown in the following example

### Target Accounts

Column: 

Application Type

 Value: 

MSSQL Azure Manager

🔍 ↻

Account N	Application Name	Application Type	Host Name	Device Name	Account Type	Owner User	Verified
sa	Azure SQL MI DB	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		✓
\${User....}	Azure SQL MI JIT	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		
\${User....}	Azure SQL MI JIT	MSSQL Azure Managed Instance	bosto...	Azure ...	Privileg...		

screenshot

OK

Cancel

#### TIP

- Accounts from the Azure SQL Managed Instance have an Application Type of "MSSQL Azure Managed Instance" and are listed by default.
- Accounts from an Azure AD have an Application Type of "Azure Access Credentials." To view such accounts, change the selection filter value to "Azure Access Credentials."
- To list all accounts, select the **Reset** icon (↻).

#### NOTE

When a user performs checkout and check-in operations using a provisioned account, their account name is replaced with either the Azure Username or the User Principal Name set in the user Extended Identity on the **Access** page.

#### TIP

**Next step:** (Optional) [Restrict Users from Editing Azure User Name Values](#).

## (Optional) Restrict Users from Editing Azure User Name Values

Most users inherit the "Manage User Azure User Name" privilege that is required to edit the Azure User Name in user definitions from their assigned role.

The following roles provide the "Manage User Azure User Name" privilege:

- Standard user
- User/Group Manager
- Delegated Administrator
- Operational Administrator
- Global Administrator
- Server Control Administrator
- UNAB Manager

For a complete list of user roles and privileges, see [User Roles](#).

**To prevent users from editing the "Azure User name" field:** Create a custom role with user privileges that do not include or inherit the "Manage User Azure User Name" privilege. For more information, see [Add or Modify Credential Manager Roles](#).

**TIP**

**Next step:** [Create an Access Policy for Azure Managed Instance JIT LDAP Users](#).

## Create an Access Policy for Azure Managed Instance JIT LDAP Users

Create an access policy that defines the device that users imported from the LDAP domain server for Azure Managed Instance Just in Time provisioning can access and the properties of that relationship.

1. Navigate to **Policies, Manage Policies**.
2. Select the **Add** button.
3. Complete the following fields on the **Association** tab of the **Add Policy** pane that opens:
  - a. **User or User Group:** Complete *one* of these fields with the Distinguished Name (DN) of the required user or group. **Tip:** Use the Search icon to display the list of choices, select the required user or group from the drop-down list, and then select **OK**.
  - b. **Device or Device Group Name:** Complete the **Device** field with the name of the device for which the policy controls access. **Tip:** Use the Search icon to display the list of choices, select the required device from the drop-down list, and then select **OK**.
4. Do the following steps on the **Password** tab:
  - a. Select the target application that you created for the provisioned account in the **Passwords** column and move it to the **Selected Passwords** column.
  - b. Select the magnifying glass icon in the **Target Account** column.
  - c. Select the target account that you created for the provisioned account and move it to the **Selected Target Account** column.
  - d. Select **OK**.
5. Select **OK** to save the policy.

## User Experience: Just in Time (JIT) Checkout and Check-in Operations

This section describes how a PAM user that has been configured in the JIT access policy checks out and checks in credentials.

1. Log into the PAM UI
2. To check out credentials for a device, do the following steps on the **Access** page:
  - a. Click the **Select** icon in the **Target Applications** column of the device entry. The name of the target application appears.
  - b. Select the account name. A **Custom Workflow Checkout Status** pane opens, showing execution details, including messages related to the directives executed along with the status of the checkout operation.

3. To check in the credentials, return to the **Access** page and select the corresponding **Check-in** link available under the **Passwords currently in use** heading. A **Custom Workflow Check-in Status** pane opens showing execution details, including messages related to the directives executed and the status of the check-in operation.

**NOTE**

If you do not check in the credentials before the checkout time limit expires, the account is checked in and all associated workflow actions are executed automatically.

## Delegate Password Management Tasks to Groups

Credential Manager uses groups to separate password management duties and improve security. Credential Manager groups allow users, or groups of users to view and change passwords for only a specific set of resources. Credential Manager users are also grouped, which simplifies the design and implementation of the security policies that are used to manage them.

**NOTE**

Credential Manager groups and roles are separate from access user groups and roles. See [Credential Manager Group Terminology](#).

**WARNING**

When defining a user that is to have Credential Manager privileges – administering or viewing passwords – the user must be assigned a Credential Manager Group. Assign a Credential Manager group by adding or editing a user from the **Users, Manage Users** screen on the **Credential Manager Groups** tab.

**NOTE**

**Important!** With release 3.4.3, the Credential Manager Role only applies to the objects scoped by the Credential Manager Target Group in the same Credential Manager Group. Previously, all Credential Manager Roles applied to all Credential Manager Target Groups in all Credential Manager Credential Groups the user was a member of.

Privileged Access Manager is preconfigured with a Credential Manager Group named "System Admin Group". This might appropriately be used to provision a Global Administrator using the PM Groups setting.

Credential Manager uses two types of groups:

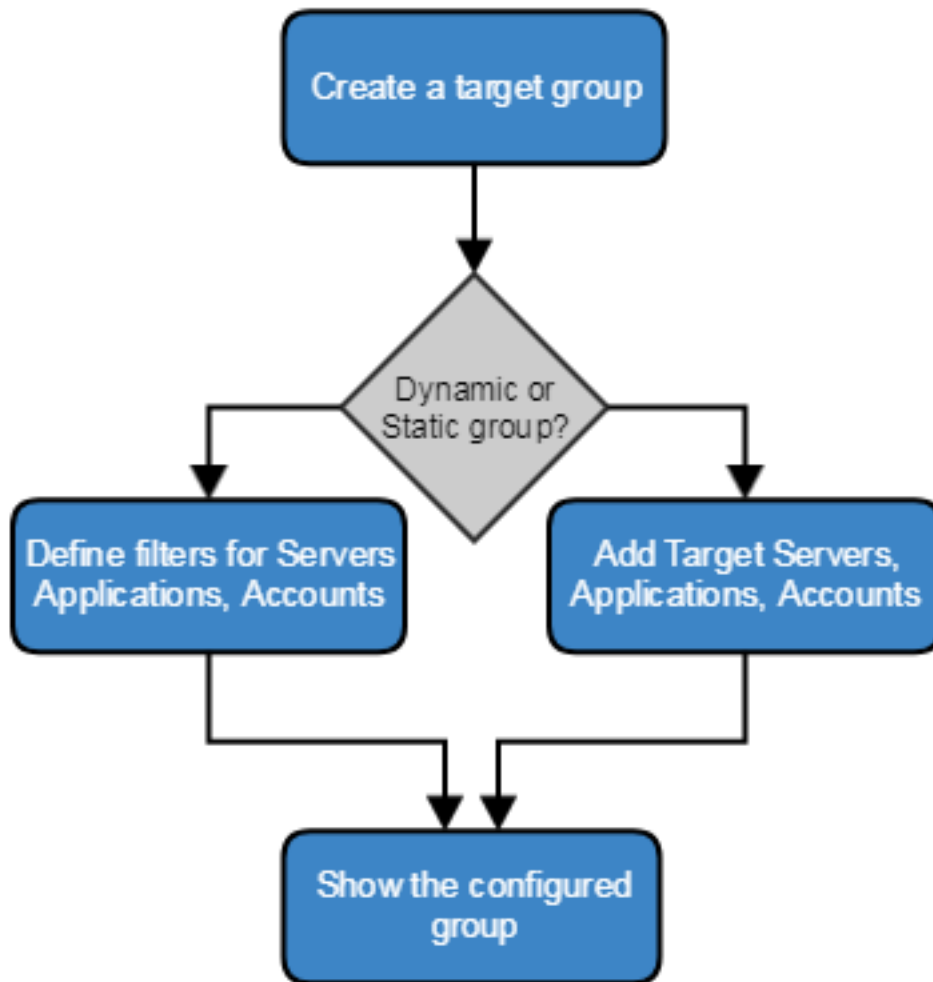
- **Static groups**

Static groups enable the direct assignment of specific resources to a particular user group. Static groups enforce the resource assignment and provide control over group membership. You can configure static target groups and A2A requestor groups.

- **Dynamic groups**

Dynamic groups use rules and filters to specify patterns for resource assignment. All entities that match the rules are assigned membership in the specified dynamic group. Any new entity that is added and that matches the pattern is automatically placed in all applicable groups, minimizing administrative burden. You can configure dynamic target groups and A2A requestor groups.

The process for defining target groups is:

**Figure 34: Credential Manager Group Configuration**

If there are no consistent standards for group attributes, names or addresses, use the Descriptor fields to create standards to support dynamic group assignment.

Authorization groupings do not apply to reports, metrics, or application-to-application credential requests.

See the following other articles in this section for more details:

- [Credential Manager Group Terminology](#)
- [Add Credential Manager Target Groups](#)
- [Add Credential Manager Requestor Groups](#)
- [Add Credential Manager Credential Groups](#)
- [Add or Modify Credential Manager Roles](#)
- [Configure Users with the Manage Credentials Privilege to View Passwords on the Access Screen](#)

## Credential Manager Group Terminology

A user or a request script can access a target account password.

- A user creates a password request from the UI, from the CLI, or from a program that uses the Java API.
- A request script executes a request to the A2A client.



To filter access to passwords, target accounts and request scripts can be organized into target groups and request groups. You can then configure credential groups to permit only selected operations on a target or request group.

### **Grouping Terminology**

The following table describes grouping terminology.

Term	Definition
Target Group	A target group is a collection of target servers, target applications, or target accounts that meet specific filter criteria. For example, all target servers that have the identifier <code>London</code> in the <code>Descriptor2</code> field. A single target can belong to multiple target groups. When a target group consists of target servers, all applications and accounts on that server are automatically contained within that target group.
Request Group	A request group is a collection of request servers (A2A Clients) or requests (scripts) that meet specific filter criteria. For example, all request servers that have the identifier <code>New York</code> in the <code>Descriptor1</code> field form a request group. A single request can belong to multiple request groups. When a request group consists of request servers, all applications on that server are automatically contained within that request group.
Roles	Each role is a collection of actions that can be performed in Credential Manager. You can build roles for each series of permissions you want to assign to users.
Credential Group	A credential group is a collection of all appliance users who are dynamically determined from a Credential Manager role, a target group, or a request group.  Credential groups are distinct and separate from Access user groups.  Specify the target group in a credential group. Then, members of the group can access any target servers, applications, or accounts. Specify the Request Group so members of the group have access to any A2A clients or scripts.
Users	Users refer to user accounts. Each Credential Manager user belongs to one or more credential groups. The credential groups define what targets and requests the user can see and what actions the user can perform on the appliance interfaces.
Filter	A condition that is assigned to a target group or request group. It determines which target or request objects are accessible by members of the target or request group.

### **Credential Manager Credential Groups and Roles**

Credential Manager credential groups and roles are distinct and separate from Access user groups and roles.

An Access user group is:

- A static association of specific users. Some user attributes, such as (Access) Roles and Access Time, can be assigned at the group level.
- Listed on the **Users, Manage Groups** page. Access user groups are created or edited from a template on that page.

A Credential Manager credential group is:

- A collection of all users who are dynamically determined from a Credential Manager role, a target group, or a request group.
- Listed on the **Credentials, Manage Credential Groups, Credential Groups** page. Credential groups are created or edited from a template that is opened on that page, or through CLI commands.

Similarly, access roles are configured with the Roles template on the **Users, Manage Roles** page. Credential Manager roles are configured on the **Credentials, Manage Credential Groups, Credential Roles** page. Credential Manager roles are created or edited from a template that is opened on that page, or through CLI commands.

**NOTE**

Be careful to avoid assigning conflicting privileges in the Credential Manager roles and Access roles for the same user or credential group. Configure segregation of duties in the Access policy, not with Credential Manager roles.

**Group Filters for Dynamic Groups**

Add filters to dynamic target and request groups to define which elements belong to the group. When using the UI to add a target or request group, you add filters from the Group List page. Filter attributes are displayed as checkboxes on the Group List page and filter types are selected from a drop-down list.

With the CLI, first add a dynamic target or request group then use the `addFilter` command to add filters.

The following table describes the filters that you can create:

Filter Object (Filter.objectClassId)	Filter Attribute (Filter.attribute)	Description
Target server (c.cw.m.ts)	Host name (hostName)	Host name for the target server.
	ipAddress (IPAddress)	IP address for the target server.
	descriptor1 (Attribute.descriptor1)	Descriptor for the target server.
	descriptor2 (Attribute.descriptor2)	Descriptor for the target server.
Target application (c.cw.m.tp)	Name (name)	Name of the target application.
	Type (type)	Type (target connector) of the target application.
	descriptor1 (Attribute.descriptor1)	Descriptor for the target application.
	descriptor2 (Attribute.descriptor2)	Descriptor for the target application.
Target account (c.cw.m.ac)	accountName (userName)	Account user name for the target account.
	accessType (accessType)	Access type for the target account.
	descriptor1 (Attribute.descriptor1)	Descriptor for the target account.
	descriptor2 (Attribute.descriptor2)	Descriptor for the target account.
request server (c.cw.m.rs)	Host name (hostName)	Host name for the request server.
	ipAddress (IPAddress)	IP address for the request server.
	descriptor1 (Attribute.descriptor1)	Descriptor for the request server.

	descriptor2 (Attribute.descriptor2)	Descriptor for the request server.
request application (c.cw.m.sc)	Name (name)	Script name for the request application.
	Type (type)	Script type for the request application.
	descriptor1 (Attribute.descriptor1)	Descriptor for the request application.
	descriptor2 (Attribute.descriptor2)	Descriptor for the request application.
	File path (filePath)	Path to the script file.
	Execution Path (executionPath)	Path from which the application is launched.

## Add Credential Manager Target Groups

A target group is a collection of target servers, target applications, or target accounts that meet specific filter criteria. For example, all target servers that have the identifier London in the Descriptor2 field. A single target can belong to multiple target groups. When a target group consists of target servers, all applications and accounts on that server are automatically contained within that target group. You can configure dynamic or static target groups.

### NOTE

**Important!:** Release 331 changed the behavior of the dynamic target group definition logic. Previously, if no filters were defined for target servers, all target servers were considered members of that filter. If neither target server nor target application filters were defined, all target applications were also considered members of the target group. For example, if you specified a filter only on an account, *all* applications and servers were added to the target group.

In 3.3.1 and future releases the following logic applies:

- If only an account filter is defined, then *only* matching accounts become members of the group; *no* servers or applications are added to the group. If you want servers or applications to belong to the group, you must *explicitly* define appropriate filters.
- If only an application filter is defined, matching applications and associated accounts are added to the group. *No* servers are added. If you want servers to belong to the group, you must *explicitly* define an appropriate filter.
- If both an account filter and an application filter are defined, matching applications and accounts from applications which match the account filter are added to the group. *No* servers are added. If you want servers to belong to the group, you must *explicitly* define an appropriate filter.

*The new logic also applies to existing dynamic target group definitions.* If this change invalidates an existing target group definition, you must manually redefine that definition so that the target group includes all the target servers, target applications, or target accounts that were previously implicitly included.

This topic covers the following contents:

### Target Group Filter Behavior Matrix

The following table shows how each combination of specified filters determines the contents of a dynamic or static target group:

Server Filter Specified	Application Filter Specified	Account Filter Specified	Objects Included in Target Group	
Yes	No	No	Matching servers, applications from the matching servers, and accounts associated with those applications.	
Yes	Yes	No	Matching servers, matching applications from the matching servers, and accounts associated with matching applications.	
Yes	Yes	Yes	Matching servers, matching applications from the matching servers, and matching accounts from the associated applications.	
Yes	No	Yes	Matching servers, applications from the matching servers, matching accounts from the included applications.	
No	No	Yes	Matching accounts only.	
No	Yes	No	Matching applications and accounts associated with those applications only.	
No	Yes	Yes	Matching applications and accounts associated with those applications only.	

### **Add Dynamic Target Groups**

Apply target group filters to target servers, target applications, or target accounts.

When you apply multiple filters to a dynamic target group, filters that use the same attribute are applied using a logical "or" relationship. For example, if a target group contains a server filter for the host name **Test** and a server filter for the host name **Production**. The group contains target servers with **Test or Production** in their host name.

Filters that use different attributes are applied using a logical "and" relationship. For example, if a group contains a server filter with the host name **Production**, and an account filter with the account name **siteAdmin**. The group contains only **siteAdmin** accounts running on servers with **Production** in the host name.

Credential Manager is preconfigured with the dynamic target group **All Targets**. The default Credential Manager Administrator account, **super**, is assigned to the All Targets group.

Credential Manager allows you to show all the targets that are associated with a specific target group. This capability allows you to validate that you have set your resource assignments and target filters appropriately.

### ***Add a Dynamic Target Group Using the UI***

Use this procedure to add a dynamic target group using the UI.

**Follow these steps:**

1. Select **Credentials, Manage Targets, Target Groups**.
2. Select **Add**.
3. Enter the group **Name**.
4. (Optional) Enter the group **Description**.
5. Select the **Dynamic** entry from the **Type** drop-down list.

**NOTE**

For AWS access accounts, the Dynamic filter does not support the Access Key Alias. The filter does support the Access Key ID.

6. Add filters to a server, application, or account. Repeat this procedure for each filter you want to add.
  - a. Select the **Not Specified** link for the filter that you want to apply. The Define Filters dialog appears.
  - b. Select **+** to add an expression.
  - c. Select the filter type (for example, contains) from the drop-down list in the **Operator** field.
  - d. Enter the filter expression (for example, 192.0.2) in the **Value** field.

When creating a filter for **Application Type**, use the following table to supply the filter expression.

**NOTE**

If you have implemented custom application types using the Target Connector Framework, those custom types will also be available from the **Application Type** drop-down menu.

Application Type	Enter the following text as the filter expression.
Active Directory	windowsDomainService
AS/400	AS/400
AWS Access Credentials Accounts	AwsAccessCredentials
AWS Proxy Credential Accounts	AwsApiProxyCredentials
Cisco	CiscoSSH
Juniper Junos	juniper
LDAP	ldap
MSSQL	mssql
MYSQL	mysql
Oracle	oracle
SPML v2.0	SPML2
UNIX	unixll
VMware ESX/ESXi	vmware
VMware NSX Controller	nsxcontroller
VMware NSX Manager	nsxmanager
VMware NSX Proxy	nsxproxy
WebLogic	weblogic10
Windows Proxy	windows

- e. Select **OK**. The Filter specification is listed.
7. After you add all your filters, select **OK** at the bottom of the page to commit the target group to Credential Manager.

**Add a Dynamic Target Group Using the CLI**

Use this procedure to add a dynamic target group using the CLI.

**Follow these steps:**

1. Add a target group. Remember to specify dynamic or static. For example:

```
Windows:
capam_command adminUserID=admin capam=mycompany.com cmdName=addGroup ^
Group.name=TokyoTargets Group.description="Targets in Tokyo" ^
Group.type=target Group.dynamic=true
Linux:
capam_command adminUserID=admin capam=mycompany.com cmdName=addGroup \
Group.name=TokyoTargets Group.description="Targets in Tokyo" \
Group.type=target Group.dynamic=true
```

2. Enter your password at the prompt. Credential Manager returns the following XML command string. Note the ID value, because it is the required Group.ID value in the addFilter command.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<Group>
<name>TokyoTargets</name>
<permissions>[]</permissions>
<type>target</type>
<readOnly>false</readOnly>
<description>Targets in Tokyo</description>
<dynamic>true</dynamic>
<ID>5</ID>
<createDate>Thu May 08 09:42:52 EDT 2008</createDate>
<createUser>admin</createUser>
<hash>eGuxUhVerHQile7mjKyW9b/ZJ04=</hash>
<updateDate>Thu May 08 09:42:52 EDT 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType />
</Group>
</cr.result>
</CommandResult>
```

3. Add a filter. For example, adding a target server host name filter:

```
Window:
capam_command adminUserID=admin capam=mycompany.com cmdName=addFilter ^
Group.ID=5 Filter.objectClassId=c.cw.m.ts Filter.attribute=hostName ^
Filter.type=contains Filter.expression="mydomain"
Linux:
capam_command adminUserID=admin capam=mycompany.com cmdName=addFilter \
Group.ID=5 Filter.objectClassId=c.cw.m.ts Filter.attribute=hostName \
Filter.type=contains Filter.expression="mydomain"
```

4. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<Filter>
<type>contains</type>
```

```

<attributeName>hostName</attributeName>
<groupID>5</groupID>
<objectClassID>c.cw.m.ts</objectClassID>
<expression>mydomain</expression>
<ID>7</ID>
<createDate>Thu May 08 09:47:35 EDT 2008</createDate>
<createUser>admin</createUser>
<hash />
<updateDate>Thu May 08 09:47:35 EDT 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType />
</Filter>
</cr.result>
</CommandResult>

```

### **Add Static Target Groups**

For static group assignments, define the specific servers, applications, and accounts that are members of the group. Static groups provide precise control over the accounts within the group.

If there are no target accounts defined for the static group, all target accounts associated with the target applications are managed.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Target Groups**.
2. Select **Add**.
3. Enter the group **Name**.
4. (Optional) Enter the group **Description**.
5. Select the **Static** entry from the **Type** drop-down list.
6. Add the servers, applications, and accounts over which the group should have control.
  - a. Select **+** for the entity you want to add. A list of available resources appears. The following figure shows a typical page that appears when you select **+** for applications
  - b. Select the desired resources from the list.
  - c. Select **OK**.

#### **NOTE**

In previous releases, selecting a specific account populated the server and application filters with the associated server and application information for that account. In 3.3.1 and future releases, you must manually add the **associated server and application**.

7. Select **OK** to save your changes.

### **View All Targets Belonging to an Existing Target Group**

Use the following procedure to view all targets belonging to an existing target group from the UI.

#### **Follow these steps:**

1. Select **Credentials, Manage Targets, Target Groups**.
2. Select the target group that you want to view and select the **UPDATE** button.
3. Select **Show**. The list of targets matching the criteria within the group displays.
4. Select **OK**.

## Add Credential Manager Requestor Groups

Learn how to add PAM Credential Manager requestor groups.

Use the following procedures to add dynamic and static requestor groups and view all requestors belonging to an existing requestor group.

### Add Dynamic Requestor Groups

For dynamic group assignments, apply requestor group filters to requestor servers and requestors. Filters provide added flexibility for defining group members.

When you apply multiple filters to a dynamic target group, filters that use the same attribute are applied using a logical "or" relationship. For example, a requester group contains a server filter for the host name **Test** and a server filter for the host name **Production**. The group contains request servers with **Test** or **Production** in their host name. Filters that use different attributes are applied using a logical "and" relationship. For example, a group contains a server filter with the host name **Production**, and an account filter with the account name **siteAdmin**. The group contains only **siteAdmin** accounts running on servers with **Production** in the host name.

Credential Manager is preconfigured with the dynamic requestor group `Requestors`. The default Credential Manager Administrator account, `admin`, is assigned to the All Requestors group.

### Applying Scripts

If you have several scripts, you can eliminate the need to provision each script manually. Set the script filters to access all client applications having a particular file or execution path. If you define Path File or Execution File filters, then all scripts in the path that meet the criteria become members of the script group. The group includes scripts that are defined in the Credential Manager database and those scripts that are not.

A credential request (`GetScriptCredentials`) can be from a script that is not defined in the Credential Manager database. Even if the script matches an authorization mapping with a requestor group, which contains the filters `Type`, `Descriptor1`, and `Descriptor2`, the credential request fails. The data for these filters does not exist in the database until the script is provisioned.

### Add Dynamic Requester Groups using the UI

Use the following procedure to add a dynamic requestor group from the UI.

#### Follow these steps:

1. Select **Credentials, Manage A2A, Request Groups**.
2. Select **Add**.
3. Enter the group **Name**.
4. (Optional) Enter the group **Description**.
5. Select **Dynamic** from the **Type** drop-down list.
6. Add filters to a client or script. Repeat this procedure for each filter you want to add to the list.
  - a. Select the **Not Specified** link for the filter that you want to apply. The Define Filters dialog appears.
  - b. Select **+** to add an expression.
  - c. Select the filter type (for example, contains) from the drop-down list in the **Operator** field.
  - d. Enter the filter expression (for example, 10) in the **Value** field.
  - e. Select **OK**.
7. Select **OK** to save your changes.

### Add Dynamic Requester Groups using the CLI

Use the following procedure to add a dynamic requestor group from the CLI.



**Follow these steps:****1. Add a requestor group. For example:**

```
Windows:
capam_command adminUserID=admin capam=mycompany.com cmdName=addGroup ^
Group.name=NewYorkRequestors Group.description="Requestors in New York" ^
Group.type=requestor Group.dynamic=true
Linux:
capam_command adminUserID=admin capam=mycompany.com cmdName=addGroup \
Group.name=NewYorkRequestors Group.description="Requestors in New York" \
Group.type=requestor Group.dynamic=true
```

**2. Enter your password at the prompt. Credential Manager returns the following XML command string. Note the ID value, because it is the required Group.ID value in the addFilter command.**

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<Group>
<ID>4</ID>
<createDate>Tue Apr 08 10:21:21 EDT 2008</createDate>
<updateDate>Tue Apr 08 10:21:21 EDT 2008</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>jrLLJH7U5QUFjNux1GDlavKk/qc=</hash>
<name>NewYorkRequestors</name>
<description>Requestors in New York</description>
<type>requestor</type>
<dynamic>true</dynamic>
<readOnly>false</readOnly>
<permissions>[]</permissions>
</Group>
</cr.result>
</CommandResult>
```

**3. Add a filter. For example, adding a requestor server host name filter:**

```
Windows:
capam_command adminUserID=admin capam=mycompany.com cmdName=addFilter group.ID=4 ^
Filter.objectClassId=c.w.m.rs Filter.attribute=hostName Filter.type=contains ^
Filter.expression="mydomain"
Linux:
capam_command adminUserID=admin capam=mycompany.com cmdName=addFilter group.ID=4 \
Filter.objectClassId=c.w.m.rs Filter.attribute=hostName Filter.type=contains \
Filter.expression="mydomain"
```

**4. Enter your password at the prompt. Credential Manager returns the following XML command string.**

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<Filter>
<ID>7</ID>
<createDate>Tue Apr 08 10:23:02 EDT 2008</createDate>
```

```

<updateDate>Tue Apr 08 10:23:02 EDT 2008</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>
</hash>
<expression>mydomain</expression>
<type>contains</type>
<objectClassID>c.cw.m.rs</objectClassID>
<attributeName>hostName</attributeName>
<groupID>4</groupID>
</Filter>
</cr.result>
</CommandResult>

```

### **Add a Static Requestor Group**

Use the following procedure to add a static requestor group from the UI.

#### **Follow these steps:**

1. Select **Credentials, Manage A2A, Request Groups**.
2. Select **ADD**.
3. Enter the group **Name**.
4. (Optional) Enter the group **Description**.
5. Select **Static** from the **Type** drop-down list.
6. Add the clients and requestors over which the group should have control.
  - a. Select **+** for the entity (Client; Script) that you want to add. A list of available resources appears.
  - b. Select one or more resources from the list.
  - c. Select **OK**.
7. Select **OK** to save your changes.

### **View All Requestors Belonging to a Requestor Group**

Credential Manager allows you to show all the requestors that are associated with a specific requestor group. You can validate that you have set your resource assignments and requestor filters appropriately.

Use the following procedure to view all requestors belonging to an existing requestor group from the UI.

#### **Follow these steps:**

1. Select **Credentials, Manage A2A, Request Groups**.
2. Select the target group that you want to view and select the **UPDATE** button.
3. Select **Show**. The list of requestors matching the criteria within the group displays.
4. Select **OK**.

## **Manage Credential Manager Credential Groups**

PAM Credential Manager credential groups (also known as Credential Manager credential groups) map a single target group to a request group and role.

To allow for flexibility, each Credential Manager administrative user can belong to multiple credential groups.

**NOTE**

After an upgrade, you may see a new credential group called Base Users. The Base Users group is a container for users that are not associated to any other user group. We recommend that you associate any Base Users to other more meaningful user groups.

The following procedures describe how to add and delete credential groups using the PAM UI, CLI, or the External API:

- [Add a Credential Group](#)
- [Delete a Credential Group](#)
- [Manage Credential Groups Using the External API](#)

**Add a Credential Group**

You can add a credential group using the PAM UI, CLI, or the External API.

**NOTE**

Be careful to avoid assigning conflicting privileges in the Credential Manager roles and Access roles for the same user or user group. Configure segregation of duties in the Access policy, not using Credential Manager roles. Currently, PAM does not support assigning more than one credential group to any single PAM user account or user group.

**Add a Credential Group Using the PAM UI**

Use the following procedure to add a Credential Manager credential group using the PAM UI.

**Follow these steps:**

1. Select **Credentials, Manage Credential Groups, Credential Groups**.  
The **Credential Manager User Groups** page opens.
2. Select the **Add** button.  
The **Add Credential Manager User Group** page opens.
3. Enter a unique **Name** for the user group.
4. (Optional) Enter a **Description** for the user group.
5. Select a **Role** with the necessary privileges. For more information, see [Add or Modify Credential Manager Roles](#).
6. Select a **Target Group**. For more information, see [Add Credential Manager Dynamic and Static Target Groups](#).
7. Select a **Request Group**. For more information, see [Add Credential Manager Request Groups](#).
8. Add credential group members using one or both of the **Users** and **User Groups** tabs. (Only users and user groups that are assigned to roles with the Manage Credentials privilege are available for selection.)

**NOTE**

You can also assign credential groups when adding or editing users and groups. For more information, see [Create and Manage Users](#) and [Configure User Groups](#).

9. Select **OK**.

**Add a Credential Group Using the CLI**

Use the following procedure to add a Credential Manager credential group Using the CLI.

**Follow these steps:**

1. Use the [addUserGroup](#) command and appropriate parameters. For example:  

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addUserGroup UserGroup.name=LonUserGroup
UserGroup.description="London user group" UserGroup.roleID=11 UserGroup.groups=3,2
```
2. Enter your password at the prompt. Credential Manager returns the following XML command string.  

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
```

```

<cr.result>
<UserGroup>
<name>LonUserGroup</name>
<readOnly>false</readOnly>
<description>London user group</description>
<role />
<roleID>11</roleID>
<groups>[]</groups>
<groupIDs>[2, 3]</groupIDs>
<ID>2</ID>
<createDate>Thu May 08 08:57:16 EDT 2008</createDate>
<createUser>admin</createUser>
<hash>D8VjG143dB45/altCCiikvXebbw=</hash>
<updateDate>Thu May 08 08:57:16 EDT 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType />
</UserGroup>
</cr.result>
</CommandResult>

```

### **Add a Credential Group Using the External API**

To learn how to use the External API to add Credential Manager user groups, see [Manage Credential Groups Using the External API](#).

### **Delete a Credential Group**

You can delete a credential group using the PAM UI, CLI, or the External API.

#### **IMPORTANT**

You cannot delete credential groups that contain users that do not belong to any other credential groups and would therefore be left without any Credential Manager privileges.

To delete such a group, do one of the following actions on each user or session manager user group that does not belong to another credential group:

- Add or move the user or group to another credential group.
- Remove all assigned Access Management roles with the Manage Credentials privilege from the user or group.

### **Delete a Credential Group Using the UI**

Use the following procedure to delete a Credential Manager credential group using the PAM UI.

#### **Follow these steps:**

1. Select **Credentials, Manage Credential Groups, Credential Groups**.  
The **Credential Manager User Groups** page opens.
2. Select the user group that you want to delete.
3. Select the **Delete** button.
4. Select the **Yes** button on the **Delete Item** dialog that appears.

#### **NOTE**

Users or access user groups with the Access Manager "Manage Credentials" privilege must belong to a credential manager user group. If deleting a Credential Manager user group would result in access users or groups no longer belonging to any user group, the deletion attempt fails with the following error message.

Error: PAM-UI-2417: Error deleting Credential Manager user group. Delete failed. The group cannot be deleted because it would leave some users of group 'example\_group' without any credential user group assigned.

## Delete a Credential Manager Credential Group Using the CLI

Use the following procedure to delete a Credential Manager credential group Using the CLI.

### Follow these steps:

1. Use the [deleteUserGroup](#) command and appropriate parameters. For example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=deleteUserGroup UserGroup.name=LonUserGroup
```

2. Enter your password at the prompt. Credential Manager runs the command and, if successful, returns something like the following example command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<UserGroup>
<name>LonUserGroup</name>
<readOnly>>false</readOnly>
<description>London user group</description>
<role />
<roleID>11</roleID>
<groups>[]</groups>
<groupIDs>[2, 3]</groupIDs>
<ID>2</ID>
<createDate>Thu May 08 08:57:16 EDT 2008</createDate>
<createUser>admin</createUser>
<hash>D8VjG143dB45/altCCiikvXebbw=</hash>
<updateDate>Thu May 08 08:57:16 EDT 2008</updateDate>
<updateUser>admin</updateUser>
<extensionType />
</UserGroup>
</cr.result>
</CommandResult>
```

### NOTE

Users or access user groups with the Access Manager "Manage Credentials" privilege must belong to a credential manager user group. If deleting a Credential Manager user group would result in access users or groups no longer belonging to any user group, the deletion attempt fails with the following error message.

Error: PAM-UI-2417: Error deleting Credential Manager user group. Delete failed. The group cannot be deleted because it would leave some users of group 'example\_group' without any credential user group assigned.

## Delete a Credential Group Using the External API

To learn how to use the External API to delete Credential Manager user groups, see [Manage Credential Groups Using the External API](#).

## Manage Credential Groups Using the External API

Use the following External API **credentialUserGroups** methods to manage credential groups.

Operation	Method	Function
POST	/cspm/ext/rest/credentialUserGroups	Add a Credential Manager User Group without users or user groups. Either id or name may be specified for each attribute. If both are specified, they must match.
PUT	/cspm/ext/rest/credentialUserGroups/{id}/users	Replace the list of Session Manager Users associated with a Credential Manager User Group. If both ids and names are supplied, they are merged. Returns the new list of members of the group using GET eligibleUsers for members only.
PUT	/cspm/ext/rest/credentialUserGroups/name/{name}/users	Replace the list of Session Manager Users associated with a Credential Manager User Group. If both ids and names are supplied, they are merged. Returns the new list of members of the group using GET eligibleUsers for members only.
PUT	/cspm/ext/rest/credentialUserGroups/{id}/userGroups	Replace the list of Session Manager User Groups associated with a Credential Manager User Group. If both ids and names are supplied, they are merged. Returns the new list of members of the group using GET eligibleUsers for members only.
PUT	/cspm/ext/rest/credentialUserGroups/name/{name}/userGroups	Replace the list of Session Manager User Groups associated with a Credential Manager User Group. If both ids and names are supplied, they are merged. Returns the new list of members of the group using GET eligibleUsers for members only.
PUT	/cspm/ext/rest/credentialUserGroups/name/{name}	Update an existing Credential Manager User Group without modifying users or user groups. The name, role, and id of the group are required. You can specify the id, name, or both for each attribute. If both are specified, they must match.
PUT	/cspm/ext/rest/credentialUserGroups/name/{name}	Update an existing Credential Manager User Group without modifying users or user groups. The name, role, and ID of the group are required. Either ID or name may be specified for each attribute. If both are specified, they must match.
GET	/cspm/ext/rest/credentialUserGroups/userName	Return all the Credential Manager User Groups that a particular Session Manager User belongs to.
GET	/cspm/ext/rest/credentialUserGroups/{id}/eligibleUsers	Return all the Session Manager Users who could be assigned to a Credential Manager User Group, along with a flag that says if they are already part of the group.
GET	/cspm/ext/rest/credentialUserGroups/userName/{name}/eligibleUsers	Return all the Session Manager Users who could be assigned to a Credential Manager User Group, along with a flag that says if they are already part of the group.
GET	/cspm/ext/rest/credentialUserGroups/{id}	Get a specific Credential Manager User Group by ID.

Operation	Method	Function
GET	/cspm/ext/rest/credentialUserGroups/{id}/protectedUserGroups	Any Session Manager User Group which belongs only to the Credential Manager User Group specified may not be removed from that group.
GET	/cspm/ext/rest/credentialUserGroups/name{name}/protectedUserGroups	Any Session Manager User Group which belongs only to the Credential Manager User Group specified may not be removed from that group.
GET	/cspm/ext/rest/credentialUserGroups/{id}/protectedUsers	Any Session Manager User which belongs only to the Credential Manager User Group specified may not be removed from that group.
GET	/cspm/ext/rest/credentialUserGroups/name{name}/protectedUsers	Any Session Manager User which belongs only to the Credential Manager User Group specified may not be removed from that group.
GET	/cspm/ext/rest/credentialUserGroups/name/{name}/eligibleUserGroups	Return all the Session Manager User Groups who could be assigned to a named Credential Manager User Group, along with a flag that says if they are already part of the group.
GET	/cspm/ext/rest/credentialUserGroups/{id}/eligibleUserGroups	Return all the Session Manager User Groups who could be assigned to a Credential Management User Group, along with a flag that says if they are already part of the group.
GET	/cspm/ext/rest/credentialUserGroups	Search for Credential Manager User Groups.
GET	/cspm/ext/rest/credentialUserGroups/name/{name}	Search for Credential Manager User Groups Get a specific Credential Manager User Group by group name.
DELETE	/cspm/ext/rest/credentialUserGroups/{id}	Delete a Credential Manager User Group by ID.
DELETE	/cspm/ext/rest/credentialUserGroups/name/{name}	Delete a Credential Manager User Group by name.

**NOTE**

When using the **credentialUserGroups** methods, consider the following information:

- **eligibleUsers** are Session Manager users with the Manage Credentials privilege.
- **eligibleUserGroups** are Session Manager user groups with the Manage Credentials privilege
- **protectedUsers** are Session Manager users that belong to exactly one Credential Manager User group besides Secrets Management Users and so cannot be removed from that other group.
- **protectedUserGroups** are Session Manager user groups that belong to exactly one Credential Manager User group besides Secrets Management Users and so cannot be removed from that other group.
- You cannot add or remove users from the following read-only Credential Manager user groups:
  - System Admin Group
  - Standard Users
  - Base Users
  - Vault Administrators
  - Secret Management Users
  - Active MQ Group

To obtain detailed information about and, optionally, test the **credentialUserGroups** methods, do the following steps:

1. If necessary, enable and configure the API Docs. See [Use the External REST API \(Programmers\)](#) for details.

2. Select **Settings, API Doc** to access the API Docs.
3. Navigate to **credentialUserGroups** to see the details of and test the available methods.

## Add or Modify Credential Manager Roles

Credential Manager roles define the privileges that a user has to perform Credential Manager functions.

### NOTE

When selecting available privileges for a role, the Credential Manager requires the associated `get` and `list` privileges. For example, if you want a user to have `addAgent` or `deleteAgent`, you must also add privileges to `getAgent`.

These following sections describe Credential Manager roles and how to manage them using the PAM UI, CLI, and External API:

- [Preconfigured Roles](#)
- [Add a Credential Manager Role](#)
- [Get Credential Manager Roles Using the External API](#)

### Preconfigured Roles

Credential Manager is preconfigured with the following roles:

- **FirecallApprover:** This role provides a user with the ability to approve password-view requests only. This role is assigned to users with a view type of General User.
- **FirecallAutoConnect:** This role is deprecated. Do not use it.
- **FirecallUser:** This role provides a user with the ability to view target account passwords only. This role is assigned to users with a view type of General User.
- **ReadOnly:** This role allows read-only access to the Credential Manager pages. Users can view information but not make any changes. Users with this role can view target account passwords. This role is distinguished from a General User role, which can view a limited subset of the Credential Manager pages.
- **RequestorAdmin:** This role provides a user privilege to access and update requestor information only. Give this role to personnel doing requestor integration for A2A integrations. Users with this role cannot add script authorizations and do not have access to any target or user information.
- **ScriptAuthorizationAdmin:** This role allows a user to add script authorizations. Give this role to personnel doing requestor integration for A2A integrations.
- **ServerAdmin:** This role provides the User access to all Credential Manager administrative functions, except those functions in Targets, Applications; Targets, Aliases; A2A or Groups menus.
- **System Admin:** The System Admin is the default role. This role has access to all Credential Manager functionality. **Do not modify this role.**
- **TargetAdmin:** This role allows a user to access and update only target information. Give this role to database administrators that register and manage database accounts using Credential Manager. Users with this role can add and update password policies; however, they cannot delete password policies. Users with this role do not have access to any requestor or user information.



### CAUTION

The TargetAdmin role includes the `updateGroup` privilege, which can be exploited by an administrator that belongs to a credential group that has the TargetAdmin role to promote their own privileges. For example, say that a target administrator user belongs to a credential group that has the TargetAdmin role that is limited by a target group (such as if the administrator is only supposed to administer accounts that belong to applications of type Oracle). However, because they have the `updateGroup` privilege, they can edit the target group to expand its scope (say to cover all target servers with an IP address that contains the digit 1).

**To prevent promotion attacks on target groups:** Create a custom role based on the TargetAdmin role that does not include any 'group' related privileges (`addGroup`, `deleteGroup`, `getGroup`, `listTargetGroup`, `updateGroup`).



Administrators with that role cannot see or manipulate target groups in any way. Alternatively, leave the privileges that allow administrators to see target groups and delete addGroup, deleteGroup, and updateGroup, and they are able to view all target groups but not be able to edit them.

- **UserAdmin:** This role allows a user to administer Credential Manager Roles and Credential Manager User Groups. This role does not allow access to targets or requestor information, nor to individual User accounts or (regular) User Groups.
- **VaultAdmin:** This role allows an administrator to view, create, update, and delete vaults and secrets across the organization. Administrators assigned this role must first be assigned the SecretsManagementUser role.

**NOTE**

The VaultAdmin role includes the addVault privilege. Any credential group that is associated with this role must include *Vaults* as the target group. Any role that has the addVault privilege does not appear under the Roles dropdown menu in the Vaults Manager window in PAM.

- **ViewReports:** This role allows a user to run some but not all of the available Credential Manager reports. More privileges are required to run the other reports.

**NOTE**

For information about what reports a user with the ViewReports role can run and which privileges are required to run the other reports, see [Credential Manager Report Roles and Privileges](#).

- **BaseRole:** This role is used internally. **Do not modify this role.**

**NOTE**

Only the FirecallUser and System Admin roles include the privileges that are required to view passwords on the **Access** screen. For information on how to configure Credential Manager administrative users to view passwords, see [Configure Users with the Manage Credentials Privilege to View Passwords on the Access Screen](#)

## **Add a Credential Manager Role**

Use one of the following methods to add a Credential Manager role:

- [Add a Credential Manager Role Using the UI](#)
- [Add a Credential Manager Role Using the CLI](#)

### ***Add a Credential Manager Role Using the UI***

Modify a role in the UI.

Follow these steps:

1. Select **Credentials, Manage Credential Groups, Credential Roles**.  
The Credential Manager Roles page appears.
2. Select **ADD**.  
The Add Credential Manager Role page appears.
3. Supply a role **Name** and **Description**.
4. Add or remove privileges using the arrows.
5. Select **OK** to save.

### ***Add a Credential Manager Role using the CLI***

Use the following procedure to add a role with the Remote CLI.

Follow these steps:

1. Add a role. For example:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addRole Role.name=patchMgrRole
Role.description="Manages patches"
Role.privileges=activatePatch,activatePatchNow,addPatch,deletePatch,deletePatchDetail,getPatchDetail,listPatch,listPatchDetail,updatePatch,updatePatchDetail,updatePatchDetailList
```

For a complete list and description of the available roles for the role.privileges parameter, see [Credential Manager CLI User Interface Actions](#).

2. Enter your password at the prompt. Credential Manager returns the following XML command string:

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success.</cr.statusDescription>
<cr.result>
<Role>
<ID>11</ID>
<createDate>Tue Apr 08 10:31:28 EDT 2008</createDate>
<updateDate>Tue Apr 08 10:31:28 EDT 2008</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>SD01a6QKWvtwUPILiY5eznW7I7I=</hash>
<name>patchMgrRole</name>
<description>Manages patches</description>
<privileges>[activatePatch, activatePatchNow, addPatch, deletePatch, deletePatchDetail, getPatchDetail,
listPatch, listPatchDetailSummary, updatePatch, updatePatchDetail, updatePatchDetailList]</privileges>
<readOnly>false</readOnly>
<hidden>false</hidden>
</Role>
</cr.result>
</CommandResult>
```

### Available Privileges for Roles

Use the following table to determine the privileges you can assign when adding or modifying a Credential Manager role.

#### NOTE

If a command is available in the CLI and the UI, the names are similar for each interface. For example, the command activatePatch is named Activate Patch in the UI. To see the complete list of UI privileges, go to [Credentials, Manage Credential Groups, Credential Roles](#). To see the complete list of CLI commands, go to [Credential Manager CLI Commands](#).

Command/Privilege Name	Interface	Description
activatePatch	UI	Sets the active flag for patches.
activatePatchDeployments	UI	Activates selected patches in the system
addAgent	UI	Adds a Credential Manager Windows Proxy.
addAuthorization	UI, CLI	Adds an authorization mapping.
addCustomWorkflow	UI, CLI	Required to create a custom workflow.
addFilter	UI, CLI	Adds a filter to a target group or request group.
addGroup	UI, CLI	Adds a target or request group.
addPasswordPolicy	UI, CLI	Adds password policies.
addPasswordViewPolicy	UI, CLI	Adds a password view policy.

addPatch	UI	Loads a Credential Manager client patch in the Credential Manager server.
addRequestScript	UI, CLI	Adds a request application.
addRequestServer	UI, CLI	Adds a request server.
addRequestServerDefaults	UI, CLI	Adds a request server default.
addRole	UI, CLI	Adds a role.
addScheduleJob	UI, CLI	Schedules a target account update or verify for later execution.
addSite	UI, CLI	Adds a site to a multisite configuration.
addSSHCertificatePolicy	UI, CLI	Adds an SSH certificate Policy to Privileged Access Manager.
addSSHKeyPairPolicy	CLI	Adds an SSH Key Pair Policy to Privileged Access Manager.
addTargetAccount	UI, CLI	Adds a target account.
addTargetAlias	UI, CLI	Adds a target alias.
addTargetApplication	UI, CLI	Adds target applications.
addTargetServer	UI, CLI	Adds a target server.
addUser	UI, CLI	Adds a user.
addUserGroup	UI, CLI	Adds a user group.
archiveAuditData	CLI	Archives audit data.
archiveMetricData	CLI	Archives metric data.
autoConnectTargetAccount	UI	Allows the user to auto-connect to a target account.
batchSequence	CLI	Provides bulk registration for CLI commands.
canGetCredentials	CLI	Validates a specified A2A request can retrieve credentials from Credential Manager.
checkConnectionStatus	UI, CLI	Checks the connection status of a client.
checkDelete	CLI (internal only)	Checks if a target server or request server can be deleted (or were previously deleted).
checkInAccountPassword	UI, CLI	Checks in an account that was previously checked out by a user viewing the password.
deleteAgent	UI	Deletes a Credential Manager Windows Proxy.
deleteAuthorization	UI, CLI	Deletes an authorization mapping.
deleteCustomWorkflow	UI, CLI	Required to delete a custom workflow.
deleteFilter	UI, CLI	Deletes a filter to a target group or request group.
deleteGroup	UI, CLI	Deletes a target or request group.
deletePasswordPolicy	UI, CLI	Deletes a password policy.
deletePasswordViewPolicy	UI, CLI	Deletes a password view policy.
deletePasswordViewRequest	UI, CLI	Deletes either a specific password view request or all expired password view requests.
deletePatch	UI	Removes a Credential Manager client patch from the Credential Manager server.
deleteRequestScript	UI, CLI	Deletes a request application.
deleteRequestServer	UI, CLI	Deletes a request server (Credential Manager client).

deleteRequestServerDefaults	UI, CLI	Deletes request server defaults.
deleteRole	UI, CLI	Deletes a role.
deleteScheduleJob	UI	Used to delete a scheduled job.
deleteSite	UI, CLI	Deletes a site from a multi-site configuration.
deleteSSHCertificatePolicy	UI, CLI	Deletes an SSH certificate policy.
deleteSSHKeyPairPolicy	UI, CLI	Deletes an SSH Key Pair policy.
deleteSystemProperty	CLI	Delete a system property (for example: set isDeleted = 1).
deleteTargetAccount	UI, CLI	Deletes a target account.
deleteTargetAlias	UI, CLI	Deletes a target alias.
deleteTargetApplication	UI, CLI	Deletes a target application.
deleteTargetServer	UI, CLI	Delete a target server.
deleteUser	UI, CLI	Deletes a user.
deleteUserGroup	UI, CLI	Deletes a user group.
disableCLIHostNameCheck	CLI	Disables Host Name verification when authenticating using the CLI.
disableFingerprinting	UI, CLI	Disables the Credential Manager client hardware fingerprinting feature.
enableCLIHostNameCheck	CLI	Forces host name checking when connecting with the CLI.
enableFingerprinting	UI, CLI	Enables the Credential Manager client hardware fingerprinting feature.
enableLicense	UI, CLI	Activates a Credential Manager license.
expirePasswordViewRequest	UI, CLI	expires a password view request.
forceCheckInAccountPassword	UI, CLI	Checks in an account that is checked out by another user.
generateEncryptedPassword	CLI	Generates an encrypted String from the value that is passed in.
generateReport	UI	Generates Credential Manager reports.
getAgent	UI	Retrieves a Credential Manager Windows proxy.
getAllScriptHash	UI, CLI	Refreshes the script hash for all the request applications on the specified request server (Credential Manager client).
getAuthorization	UI	Retrieves an authorization mapping.
getAwsManagementConsoleSessionUrl	CLI	Retrieves a URL to an authenticated Amazon Web Services Management Console federation session.
getErrorCodes	CLI	Retrieves the list of Credential Manager server error codes.
getEventProcessingMetrics	CLI	Gets metrics for notification event processing.
getGroup	UI	Retrieves a target group or request group.
getLocalProperty	CLI	Retrieves the property value which matches the property name.
getLogs	UI, CLI	Retrieves a ZIP file containing the logs from a siteServer or requestServer.
getMetric	UI	Retrieves metric data.
getMostRecentPasswordHistory	Internal	Retrieves the most recent password history for a target account.

getMSOLFederatedSessionCmd	CLI	Generates a federated session request for presentation to the MSOL portal. The request is returned as a web form that is automatically submitted by the browser. Submitting the form launches a federated session with MSOL.
getNumberOfAccounts	UI, CLI	Retrieves the number of target accounts that are registered in Credential Manager.
getPasswordHistory	UI	Retrieves the password history for a target account.
getPasswordViewPolicy	UI	Retrieves a single password view policy from the DB by ID or name
getReportData	UI	A command to retrieve data for a named report
getRequestServerDefaults	UI, CLI	Gets request server defaults.
getScheduleJob	UI	Gets a scheduled job.
getScript	UI	Retrieves a request application.
getScriptHashAsynchronous	UI, CLI	Refreshes the script hash for a specified request script on a request server (Credential Manager client).
getServiceStatus	CLI	Gets the status of services that are associated with a Windows Domain Service target account. This command assumes that the service information is stored in the extend attribute serviceInfo.
getSite	UI	Retrieves a site.
getSystemProperty	CLI	Retrieves the property value which matches the property name.
getTargetAccount	UI	Retrieves a target account.
getTargetAlias	UI	Retrieves a target alias.
getTargetApplication	UI	Retrieves a target application.
getTargetServer	UI	Retrieves a target server.
getUser	UI	Retrieves a user.
getUserGroup	UI	Retrieves a user group.
listAuthorization	UI	Lists authorization mappings.
listDBClusterMembers	UI, CLI	Lists database cluster members in the system.
listGroups	UI	Lists user groups.
listMetrics	UI	Retrieves metric data.
listPasswordHistory	UI	Lists the password history for target accounts.
listPasswordViewRequestByApproverSummary	UI, CLI	Returns a list of password view requests for an approver.
listPasswordViewRequestByRequestorSummary	UI, CLI	Returns a list of password view requests for a requestor.
listPasswordViewRequestSummary	UI	Returns a list of password view requests.
listPatch	UI	Lists the Credential Manager client patches loaded in the Credential Manager server.
listPatchDeploymentSummary	UI	Lists the patch deployments.
listReports	UI	Lists the available reports.
listRequestScript	UI	Lists request applications.

listRequestServerDefaults	CLI	Lists Request Server defaults.
listScheduleJob	UI	Lists scheduled password validation and updates.
listTargetAccounts	UI	Lists target accounts.
listTargetAliases	UI	Lists target aliases.
listTargetApplications	UI	Lists target applications.
listUsers	UI	Lists Credential Manager users.
readCustomWorkflow	UI, CLI	Required to read a custom workflow.
renameUser	CLI	Creates a copy of an existing user with a new name, and deletes the old user.
resetClientCache	CLI	Informs all active clients that their caches of saved passwords should be reset. Contact CA Support before using this command.
resetDBHash	UI, CLI	Resets the database hash for an object.
resetGroupCache	CLI	Resets the group cache for all groups, or a single group. This command is asynchronous.
searchAgent	CLI	Lists Credential Manager Windows Proxies.
searchAuditLog	UI	Lists audit log records.
searchAuthorization	CLI	Lists authorization mappings.
searchCustomWorkflow	UI, CLI	Required to search and list custom workflows.
searchFilter	UI, CLI	Lists filters.
searchGroup	CLI	Lists target groups or request groups.
searchPasswordPolicy	CLI	Lists Password Composition Policies.
searchPasswordViewPolicy	UI, CLI	Lists password view policies in the system.
searchPasswordViewRequest	UI, CLI	Lists the password view requests in the system.
searchPasswordViewRequestByApprover	UI, CLI	Lists the password view requests for a particular approver. The approver is the user executing the command.
searchPasswordViewRequestByRequestor	UI, CLI	Lists the password view requests for a particular requestor. The requestor is the user executing the command.
searchRequestScript	CLI	Lists request applications.
searchRequestServer	UI, CLI	Lists request servers.
searchRole	CLI	Lists roles.
searchServerKey	UI	Lists all the server keys.
searchSite	UI, CLI	Lists sites.
searchSSHCertificatePolicy	UI, CLI	Lists SSH certificate policies.
searchSSHKeyPairPolicy	CLI	Lists SSH Key Pair policies.
searchTargetAccount	CLI	Lists target accounts.
searchTargetAlias	CLI	Lists target aliases.
searchTargetApplication	CLI	Lists target applications.
searchTargetServer	UI, CLI	Lists target servers.
searchUser	CLI	Lists users.
searchUserGroup	CLI	Lists user groups.

setInitProperty	CLI	Sets the initialization property (database username and password) for DB2 databases.
setLocalProperty	CLI	Sets the site name in the site-local Credential Manager data store.
setPasswordViewReasons	CLI	Sets the password view reasons text for UI display.
setPasswordViewRequestDeleteInterval	UI, CLI	Sets the Password View Request Delete Interval.
setReportRowLimit	UI, CLI	Sets the maximum number of entries that reports display.
setSystemProperty	CLI	Sets a Credential Manager system property.
showGroup	UI	A command that retrieves the contents of a Requestor or Target group.
updateAgent	UI	Changes a Proxy.
updateAuthorization	UI, CLI	Changes an authorization mapping.
updateCompoundServers	UI	Changes a target compound server.
updateCustomWorkflow	UI, CLI	Required to update a custom workflow.
updateDBClusterMembers	UI, CLI	Update information about a database cluster member.
updateDBPassword	CLI	Changes the Credential Manager datastore administrator password on all databases except DB2.
updateFilter	UI, CLI	Updates a filter in a target group or request group.
updateGroup	UI, CLI	Changes target and request groups.
updatePasswordHistory	UI	Changes a password history item.
updatePasswordPolicy	UI, CLI	Updates password policies.
updatePasswordViewPolicy	UI, CLI	Updates a password view policy.
updatePasswordViewRequestStatus	UI, CLI	Updates the status of password view request to 'approved' or 'denied'.
updateRequestScript	UI, CLI	Changes a request application.
updateRequestServer	UI, CLI	Changes a request server.
updateRequestServerDefaults	UI, CLI	Updates a request server defaults.
updateRequestServerKey	UI, CLI	Changes a request server (Credential Manager client) encryption key.
updateRole	UI, CLI	Changes a role.
updateServerKey	CLI	Changes the Credential Manager server encryption key.
updateSite	UI, CLI	Changes site information.
updateSSHCertificatePolicy	UI, CLI	Updates an existing SSH certificate in Privileged Access Manager.
updateSSHKeyPairPolicy	CLI	Updates an existing SSH Key Pair Policy in Privileged Access Manager.
updateTargetAccount	UI, CLI	Changes a target account.
updateTargetAccountDescriptor	CLI	Changes a target account descriptor value.
updateTargetAccountPassword	UI, CLI	<p>Changes a target account password.</p> <p><b>Note:</b> To change passwords using the UI, this Role also requires the updateTargetAccount permission.</p> <p>The CLI only requires the updateTargetAccountPassword permission to change passwords.</p>

updateTargetAlias	UI, CLI	Changes target aliases.
updateTargetApplication	UI, CLI	Changes target applications.
updateTargetServer	UI, CLI	Changes target servers.
updateUser	UI, CLI	Changes user information.
updateUserGroup	UI, CLI	Changes a user group.
updateUserPassword	CLI	Changes a user password.
updateUserStatus	UI, CLI	Enable or disable access of a Credential Manager user to the system.
verifyAccountPassword	UI, CLI	Verifies a synchronized account password or all synchronized accounts in a target group (optionally excluding verified or non verified accounts).
verifyDBHash	CLI	Verifies the hash value of most BaseModel objects that are stored in DB.
viewAccountPassword	UI, CLI	Allows the user to view an account password.

### Get Credential Manager Roles Using the External API

Use the External API **credentialRoles** method to get Credential Manager roles.

Operation	Method	Description
GET	/cspm/ext/rest/credentialRoles	Get Credential Manager roles.

To obtain detailed information about and, optionally, test the **credentialRoles** method, do the following steps:

1. If necessary, enable and configure the API Docs. See [Use the External REST API \(Programmers\)](#) for details.
2. Select **Settings, API Doc** to access the API Docs.
3. Navigate to **credentialRoles** to see the details of and test the method.

## Configure Users with the Manage Credentials Privilege to View Passwords on the Access Screen

By default, users with Credential Manager administrative privileges do *not* have privileges to view passwords on the **Access** screen. This article describes how to create and assign a Credential Manager group with password viewing privileges.

### NOTE

**Background:** By default, users are assigned to the "[Standard User](#)" role and are *silently* assigned to the "Standard Users" Credential Manager group. ("Standard Users" is not shown on the **Credential Manager Groups** tab). Membership of the "Standard Users" Credential Manager group provides privileges to view account passwords on the **Access** page. However, when a user is assigned any role with the "Manage Credentials" privilege (for example, "Password Manager"), that user is removed from the "Standard Users" Credential Manager group and cannot view passwords on the **Access** page.

### Follow these steps:

1. Do the following steps to create the Credential Manager role:
  - a. Open **Credentials, Manage Credential Groups, Credential Roles**.
  - b. Select **ADD**.
  - c. Enter a **Name** for the new role. For example, "ViewPasswords."



- d. Move the following privileges from the **Available Privileges** column to the **Selected Privileges** column:

- Get Password View Policy
- Get Target Account
- View Account Password

The following screenshot shows an example:

**Add Credential Manager Role**

Name:

Description:

**Available Privileges**

- ☐ Name
- ☐ Update Server Key
- ☐ Update Site
- ☐ Update Target Account
- ☐ Update Target Account Descriptor
- ☐ Update Target Account Expired Password
- ☐ Update Target Account Password
- ☐ Update Target Alias
- ☐ Update Target Application
- ☐ Update Target Server
- ☐ Update User
- ☐ Update User Group
- ☐ Update User Password
- ☐ Update User Status
- ☐ Verify Account Password
- ☐ Verify DB Hash

**Selected Privileges**

- ☒ Name
- ☒ Get Password View Policy
- ☒ Get Target Account
- ☒ View Account Password

**OK** **CANCEL**

- e. Select **OK** to save the role and exit.
2. Do the following steps to create a Credential Manager group with the "ViewPasswords" role that you created in Step 1:
- Open **Credentials, Manage Credential Groups, Credential Groups**.
  - Select **ADD**.
  - Enter a **Name** for the new group. For example, "View Passwords."
  - Select the "ViewPasswords" role that you created in Step 1 from the **Role** drop-down list.
  - Add a **Target Group**. Note that if user A is assigned a credential manager group with the "Target Administrator" role and "Targets" as the target group, that user sees only the assigned "Targets" group in the display, not other target groups. User A can add a new target group, but it does not appear in the display because user A does not have the permissions to view it. To see other groups, assign the user A with the Credential Manager group with the "Target Administrator" role only.
  - Optionally, add a **Request Group** for A2A.

The following screenshot shows an example:

## Update Credential Manager User Group View Passwords

?
✕

---

Basic Info

Users

---

Name: \*

View Passwords

Description:

Add to an Access user to allow users to view passwords on the Access screen.

Role: \*

ViewPasswords

🔍

Target Group:

Targets

🔍

Request Group:

Requestors

🔍

OK

CANCEL

- g. Select **OK** to save the group and exit.
3. Do the following steps to add the "View Passwords" group that you created in Step 2 to the user account with Credential Manager administrative privileges:
  - a. Open **Users, Manage Users**.
  - b. Select the user account with Credential Manager administrative privileges and select **UPDATE**.
  - c. Select the **Credential Manager Groups** tab.
  - d. Move the "View Passwords" group that you created in Step 2 from the **Available Groups** column to the **Selected Groups** column.

The following screenshot shows an example user with Report Viewer and View Passwords Credential Manager groups:

**Update User Pat**

Basic Info Administration Roles Access Times Groups **Credential Manager Groups** API Keys

Available Groups

- ☐ Name
- ☐ AWS Proxy Accessors
- ☒ Base Users
- ☐ NSX Proxy Accessors
- ☐ NewNewRole
- ☐ Passwords and reports
- ☐ Standard Users
- ☐ System Admin Group

Selected Groups

- ☐ Name
- ☐ Report Viewer
- ☐ View Passwords

MANAGE POLICY

OK CANCEL

e. Select **OK** to save the user and exit.

The user can now see passwords on the **Access** screen.

## Configure a PAM User to View the Password History of Target Accounts

Use this procedure to learn how to view the Target Account's password credential history.

**Follow these steps:**

1. [Add a new Credential Manager Role](#) named **CredentialHistory**.

2. Add the following privileges: **Get Password History**, **Get Target Account**, **List Password History**, **List Target Accounts**, and **Search Target Account**.

### Update Credential Manager Role CredentialHistory

Name: \*

Description:

Available Privileges

- ☐ Name
- ☐ Activate Patch
- ☐ Activate Patch Deployments
- ☐ Add A2A Client
- ☐ Add A2A Client Defaults
- ☐ Add A2A Script
- ☐ Add Agent
- ☐ Add Authorization
- ☐ Add Filter
- ☐ Add Group
- ☐ Add Password Policy
- ☐ Add Password View Policy
- ☐ Add Patch
- ☐ Add Policy
- ☐ Add Role

Selected Privileges

- ☐ Name
- ☒ Get Password History
- ☐ Get Target Account
- ☐ List Password History
- ☐ List Target Accounts
- ☐ Search Target Account

OK

3. [Add a new Credential Manager Group](#) named **Credential History Accessors** with the **CredentialHistory** role, and the appropriate **Target Group**. **Note:** *Targets* by default provides access to credentials across all Target Devices. To restrict viewing credentials to certain Target Devices, create a new Target Group that only

includes the desired Target Devices. A **Request Group** is not needed.

4. [Create a new user.](#)
5. Under **Roles**, remove the automatically assigned **Standard User Role**. This prevents the **Access** page from loading on login.
6. Add the **Password Manager** role.

7. Under the **Credential Manager Groups** tab, add the **Credential History Accessors CM Group**, and click OK to complete and confirm this page.

8. **Note:** At this point, **log in** as the newly-created user to view credential history directly from the **Target Accounts** page.
9. Select the desired **Target Account** to view its credential history.

Account Name	Application Name	Application Type	Host Name	Device Name	Account Type	Owner User Name	Verified	Action
CA7apApUser...	ApiKey	XsaultApiKey	apikeyxcedu...	apikeyxcedu...	AQA		✓	
MCapiKey-1001	ApiKey	XsaultApiKey	apikeyxcedu...	apikeyxcedu...	AQA		✓	
nimadmin	CA Normaliza...	CalimSM	nim.pam.ca.c...	nim.pam.ca.c...	Privileged			
nimadmin	CA Normaliza...	CalimJM	nim.pam.ca.c...	nim.pam.ca.c...	Privileged			
root	SSHDevice-76	ssh	10.17.45.199	SSHDevice	Privileged			

- **To view the Target Account's password history**, select the **Credential History** icon located next to the Password field. **Note:** Such a user can perform NO OTHER action on this page, as the user only

has privileges to view password history. For example, clicking the magnifying glass by the **Host Name**, **Application Name**, or **Password View Policy** fields displays a permission error, as the user does not have the proper privileges. Lack of permissions also disallows viewing the current credential of the Target Account.

- The **Password History** is a list of all previous credentials for this Target Account, ordered by **Date**

Date Changed	Changed By	Compromised
2020/04/01 11:21:34 GMT-0000	super	<input type="checkbox"/>
2020/04/01 11:21:22 GMT-0000	super	<input type="checkbox"/>
2020/03/26 13:10:37 GMT-0000	super	<input type="checkbox"/>
2020/03/25 13:04:35 GMT-0000	super	<input type="checkbox"/>
2020/03/25 13:04:06 GMT-0000	super	<input type="checkbox"/>
2020/03/25 13:03:58 GMT-0000	super	<input type="checkbox"/>

Changed.

- To view the actual historical password for the Target Account at a particular date, select the desired entry in the Password History list.

."/>

## Manage Credentials Between Applications (A2A)

The A2A (Application to Application) feature lets you manage credential requests from automated request servers. After Credential Manager provides the password, the request server submits them to access the target. *Request scripts* are applications that require credentials for target accounts on password management target devices. These scripts request the managed credentials by way of the A2A Client, which runs on a request server. This request server is treated like a target server but is an A2A device type.

The A2A feature uses an A2A Client that you install on a host in the customer environment. The A2A Client then has to integrate with the appliance.

This topic describes the following tasks:

### A2A Terminology

The following terms are specific to A2A configurations:

- **Request Server:** A host server where the requestor application resides and where you install the A2A Client.
- **A2A Client:** A program that is installed on the request server. The A2A is the intermediary that communicates between the requestors and PAM.
- **Requestor:** A program or script that requests credentials that are stored as part of an A2A target account at PAM. To obtain credentials, the requestor communicates to the A2A Client, which then fetches the credentials from PAM. When PAM receives the credential request, it evaluates attributes of the request server, the requesting program/script, and the user executing the requesting program. If authorized, PAM sends the credentials to the requestor. A requester can use credentials for any task that requires credentials, such as opening connections to databases.
- **Target Alias:** A unique name that identifies an A2A target account. An A2A target account might have multiple aliases.
- **Authorization Mapping:** A mapping defines which requesting application or scripts can access which target accounts. Mappings implement A2A security.

## **Configuration Overview**

This section provides a high-level overview of the process to configure A2A credential management:

### **NOTE**

You do not have to complete the A2A tasks in any specific order. The only exception is for A2A deployments on an AWS AMI in an Amazon Virtual Private Cloud.

1. Add target devices that host target accounts for use by request servers. These targets use the device type Privileged Management.
2. Install the A2A Client on a remote host.
3. Use the PAM UI to register the A2A Client with a PAM server or a site VIP in a clustered environment.
  - a. Add the A2A Client as an A2A device.
  - b. Activate the Device.
4. Integrate the A2A request scripts on the A2A Client host
5. Use the UI and integrate the request server with the appliance server:
  - a. Specify the A2A request scripts
  - b. Specify authorization mappings

## **Configure A2A for High-Availability in Multisite Clustered Environments**

You can configure your A2A implementation to provide varying levels of availability in a multisite clustered environment by configuring the PAM nodes at which sites to which each request server can connect. The more PAM nodes to which a request server can connect, the higher the availability.

At a minimum, configure each request server to be able connect to all the PAM nodes at its site by taking the following actions:

- Register all request servers with their local site VIP, not an individual PAM node.
- Configure your network and firewall rules to provide all PAM nodes at a site with a clear network path to all locally registered request servers.

### **NOTE**

The previous configuration is considered the default solution and is used in all associated procedures in this documentation.

Example configurations for higher A2A availability:

- **For additional A2A availability:** Configure your environment so that each request server has a clear network path to every PAM node at its local site *and* the primary site.
- **For maximum A2A availability:** Configure your environment so that each request server has a clear network path to every PAM node in your cluster

**IMPORTANT****High-Availability vs. Security and Performance**

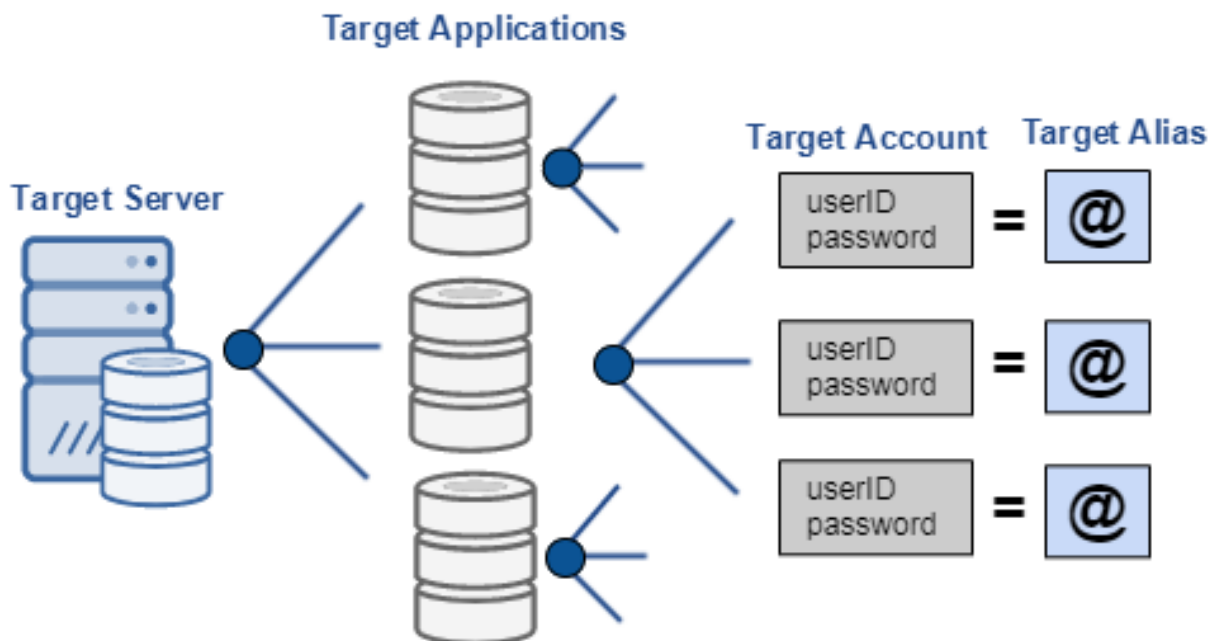
Because higher availability configurations require more connections between request servers and PAM nodes, some at remote sites, there is a corresponding impact on network security and performance. Configuring network and server firewall rules to allow the associated connections affects network security. The additional network traffic affects network performance. You must therefore consider these trade offs when determining your availability strategy.

**Identify Targets Using Target Aliases**

To manage A2A passwords, assign one or more target aliases for each target account. A target alias is a unique name that links a target server, a target application on that server, and a target account for that application. A script that is integrated with Credential Manager, uses the alias to retrieve the target account credentials from the database. The credentials enable access to the target system. With a target alias defined, target credentials are not hard-coded into scripts, allowing Credential Manager to handle password changes automatically.

The following figure shows the hierarchical structure of target accounts.

**Figure 35: Target Aliases for A2A Communication**



Requesting programs also identify a target account by specifying a target alias. Target aliases are global to the appliance. The aliases differ from target account names because target names can be duplicated on many hosts. An example of a duplicated name is the root account on UNIX systems.

Target aliases and groups are also used in authorization mappings.

Specifying a target alias is identical to the target alias specified by the requesting program.

If the mapping is to a target group, all accounts in the group represent the target. Grouping targets lets the requesting program/script obtain the target aliases for each target account without you configuring multiple mappings. Target groups are the most scalable way of specifying targets. However, some requesting programs might get credentials for target accounts that are not needed. To prevent this issue, configure mappings to individual aliases or set up target groups with the smallest scope possible.



**TIP**

See the following related content for more information about configuring A2A to allow PAM to manage credential requests from automated request servers:

- [Install and Activate an A2A Client on a Request Server](#)
- [Target Aliases for A2A Target Accounts](#)
- [Start or Stop an A2A Client](#)
- [A2A Client Connection Security](#)
- [Integrity Verification](#)
- [Add A2A Requestors](#)
- [Configure A2A Authorization Mappings](#)
- [View Unsuccessful A2A Client Requests](#)
- [Run an Example Application](#)
- [Modify the A2A Client Configuration File](#)
- [View A2A Client Logs](#)
- [Update an A2A Client Key](#)
- [Check A2A Client Connection Status](#)
- [Configure an A2A Client to Use Another Server](#)
- [Configure the A2A Client Multi-Home Feature](#)
- [Configure A2A Client Event Polling](#)

## Install and Activate an A2A Client on a Request Server

The A2A Client manages the connection between Privileged Access Manager and a request server. The A2A Client runs on a request server and allows requestors to communicate securely with the appliance.

This topic describes the requirements and installation procedures for an A2A Client.

### **A2A Client Hardware Requirements**

The following table details the hardware requirements for the A2A Client.

A2A Client	Hardware Requirements
A2A Client (32-bit)	32-MB RAM 120-MB hard drive space
A2A Client (64-bit)	32-MB RAM 170-MB hard drive space

50 MB must also be reserved for the A2A Client log file.

### **A2A Client Operating System Requirements**

The A2A Client runs as a daemon or service and requires a Java Virtual Machine (JVM). The A2A Client can be installed on 32-bit and 64-bit operating systems.

**NOTE**

The 32-bit installation is no longer supported on Linux or Solaris Sparc systems. However, the 32-bit **libcwjcafips.so** file is preserved as **libcwjcafips32.so** so that you can still run your applications using a 32-bit JRE if necessary.

To use the 32-bit **libcwjcafips32.so** file, follow these steps:

1. Navigate to **/citech/cspmclient/lib**.

2. Copy **libcwjcafips32.so** to a different folder.
3. Rename **libcwjcafips32.so** to **libcwjcafips.so**.
4. Set the **java.library.path** to point to the folder that contains your new **libcwjcafips.so** file before pointing to the **/catech/cspmclient/lib** folder.

### **Prepare the Request Server System for A2A Client Installation**

Before you install the A2A Client, do the following tasks:

- **Important!** Verify that no A2A Client is already installed on the host system. If there is, uninstall it. For more information, see [Uninstall the A2A Client](#).
- Verify that all A2A Client hardware and software requirements are met.
- Ensure that firewalls do not block the necessary communication ports. See [Default Port Settings](#) for details.
- Verify that the A2A Client correctly resolves the PAM appliance name using DNS. If DNS resolution fails, correct the issue. If it cannot be corrected, place the name in the A2A Client host file:
  - **On UNIX:** `/etc/hosts`
  - **On Windows:** `C:\Windows\System32\drivers\etc\hosts`
- Verify that the appliance resolves the DNS name of the A2A Client host. From the UI, select **Configuration, Tools**. Try to resolve the name of the A2A Client host. If it does not resolve, then correct the issue.

#### **TIP**

You can also verify DNS resolution after the A2A Client is started using the following procedure in the PAM UI:

1. Select **Credentials, Manage A2A, Mappings**.
  2. Select **Add** then use the magnifying glass for the **Request** field to display a list of A2A Clients.
  3. Verify that your A2A Client is displayed.
- The default installation directory for the A2A Client is one of the following:
    - **Windows:** `C:\cspm`
    - **Standard UNIX install:** `/opt/cloakware`
    - **RPM-based install for RHEL:** `/opt/Broadcom/PAM/A2A`
- If you do not want to use the default directory, create an alternate installation directory.

### **Download the A2A Client Software**

Download the A2A Client software from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

### **Install the A2A Client**

You can install the A2A Client on a UNIX or Windows host.

- [Install the A2A Client on a Windows Host](#)
- [Install the A2A Client on a UNIX or Linux Host Using the Install Script](#)
- [Install the A2A Client on a RHEL Host Using the RPM Package](#)
- [Install the A2A Client on an AIX Host](#)
- [Deploy an A2A Client on an AWS AMI](#)

#### ***Install the A2A Client on a Windows Host***

Install a single A2A Client on the Windows host. Multiple Clients on the same host are not supported. If there is an existing A2A Client, uninstall it before proceeding.

If the A2A Client host is a 64-bit platform, you can install the 32-bit or the 64-bit A2A Client. Install the 64-bit client to integrate with 64-bit applications or the 32-bit client to integrate with 32-bit applications.

### NOTE

The A2A Client installation on Windows is performed by InstallAnywhere software. If you execute the installation from an account that contains special characters, the InstallAnywhere wizard fails. To avoid this problem, start the installation by right-clicking on the executable file and selecting the **Run As** option. The **Run As** dialog opens and prompts for an alternate username and password for the installation. Specify the account credentials and continue with the installation.

### Follow these steps:

1. Open a Command window and navigate to the `clients/win` subdirectory in the unzipped installation package.
2. Start the installation wizard by double-clicking  
`setup_windows32_java.exe`  
or  
`setup_windows64_java.exe`  
An InstallAnywhere window informs you that the installation preparation has started.  
When the preparation completes, the A2A Client Welcome window followed by the **Introduction** window. Select Next.
3. In the **Choose Install Folder** window, enter, or select the folder where you want to install A2A Client.  
Do not use a space in the installation folder names.
4. In the **Server Information** window, specify one of the following options in the **Server Name** field:
  - **Clustered environment:** The IP address or fully qualified domain name (FQDN) of a node at the nearest site or the site VIP if there is one. If you specify the FQDN, it must match the name in the appliance SSL certificate.
  - **Unclustered environment:** The IP address or fully qualified domain name (FQDN) of the PAM server.

### NOTE

#### Important Information:

- In a clustered environment, always specify the address of the site VIP, if available. The VIP provides automatic load-balancing and failover between all the nodes at that site.
  - The specified `server_address` value is written to the A2A Client configuration file (`CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`).
  - In a multisite cluster, add alternate site VIPs or node addresses to the A2A Client configuration file to configure A2A Client failover. For more information, see [Configure A2A Client Failover upon Connection Failure in a Cluster](#).
5. Optionally enable IPv6 by checking the **IPV6 Enabled** checkbox.
  6. In the **Choose Log Directory** window, enter a specific path name for the installation log file directory or use the default path name.
  7. In the **Pre-Installation Summary** window, validate the installation information then select **Install**.  
The **Installing Password Authority Client** window appears and shows the progress of the installation.
  8. When the installation finishes, the **Install Complete** window appears. Select **Done**.
  9. Do *one* of the following tasks to auto-register the A2A Client by starting the PAM software component service:
    - Open a command window and enter: `net start cspmclientd`
    - Open the Windows Services tool and start the `cspmclientd` service.

After the installation is complete and the client is started, the Client registers with PAM.

### **Install the A2A Client on a UNIX or Linux Host Using the Install Script**

Run the install script on *each* request server to install the A2A Client.

### NOTE

This release also includes an RPM package for use with Red Hat Enterprise Linux (RHEL) hosts. For more information, see [Install the A2A Client on a RHEL Host Using the RPM Package](#).

Install and configure the A2A Client on all request servers, but install only one A2A Client on each host. If there is an existing A2A Client, uninstall it before proceeding.

#### NOTE

Before you install the A2A Client on a Linux system, ensure that your system has the correct 32-bit or 64-bit libidn installed. If you try to install the Client without the correct libidn. The installation stops and an error message is displayed.

#### Follow these steps:

1. Open a shell window and navigate to the location of the unzipped A2A Client installation package:

```
cd unzip_location/
```

2. Enter the following command:

```
chmod u+x setup_unix
```

3. Start the installation script by entering the following command and options:

```
./setup_unix host_type A2A_client_install_dir  
server_address [true|false]
```

Where:

- *host\_type*: The type of UNIX host. Enter `Linux` or `SolarisSparc`
- *A2A\_client\_install\_dir*: The complete pathname of the installation directory for the A2A Client software. Relative path names (that is, paths beginning with `./`) are not acceptable.
- *server\_address*: One of the following options:
  - **Clustered environment**: The IP address or fully qualified domain name (FQDN) of a node at the nearest site or the site VIP if there is one. If you specify the FQDN, it must match the name in the appliance SSL certificate.
  - **Unclustered environment**: The IP address or fully qualified domain name (FQDN) of the PAM server.
- *[true/false]*: Optionally enable IPv6

#### NOTE

##### Important Information:

- In a clustered environment, always specify the address of the site VIP, if available. The VIP provides automatic load-balancing and failover between all the nodes at that site.
- The specified *server\_address* value is written to the A2A Client configuration file (`CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`).
- In a multisite cluster, add alternate site VIPs or node addresses to the A2A Client configuration file to configure A2A Client failover. For more information, see [Configure A2A Client Failover upon Connection Failure in a Cluster](#).

4. Auto-register the A2A Client (request server) in the GUI by starting the daemon. Enter the following command:

```
cspmclientd start
```

After the installation is complete and the client is started, the client registers with PAM.

#### (Optional) Install the A2A Client on a Red Hat Enterprise Linux Host Using the RPM Package

You can install Red Hat A2A Clients using the standard UNIX install script. However, using the available RPM package with a Red Hat native package manager (YUM or DNF) to install the client provides the following benefits:

- To support efficient installation of the A2A Client on multiple request servers, you can place the RPM package in a central repository of a package handler rather than download it to each host.
- Package handlers can identify from the RPM that the A2A Client requires the **libidn** library and can resolve this dependency by installing the correct version automatically, if necessary. (You have to do this manually when using the standard UNIX install script.)
- Package handlers can identify an existing A2A Client that was installed from an RPM package and can upgrade it automatically. A2A Clients that are installed using the UNIX install script do not support upgrades and must be **manually uninstalled before installing the new version**.

#### NOTE

You can also obtain the same benefits using a more sophisticated software automation tool, such as Ansible or Jenkins.

The following content assumes that you are familiar with your choice of package manager or software automation tool and therefore only provides the information that you require.

- The RPM file name is `LinuxA2A-version-1.x86_64.rpm`.

#### NOTE

If you are using a package manager repository, add the `LinuxA2A-version-1.x86_64.rpm` to that repository.

- Use one of the following options to specify the address (FQDN or IP address) that the A2A Client uses to communicate with PAM:
  - Set a **PAM\_SERVER** environment variable before installation. The corresponding value in the A2A Client configuration file is populated automatically.
  - Edit the `<cspmserver>server_address</cspmserver>` parameter in the A2A Client configuration file (`/opt/Broadcom/PAM/A2A/cspmclient/config/cspm_client_config.xml`).
  - Copy a correctly configured A2A Client configuration file to the `/opt/Broadcom/PAM/A2A/cspmclient/config` directory on all A2A Client hosts after installing them from local files or a repository.

In either case, specify the appropriate address for your environment:

- **Clustered environment:** The IP address or fully qualified domain name (FQDN) of a node at the nearest site or the site VIP if there is one. If you specify the FQDN, it must match the name in the appliance SSL certificate.
- **Unclustered environment:** The IP address or fully qualified domain name (FQDN) of the PAM server.
- Optionally (a default value of 28088 is preconfigured), use one of the following options to specify the port that the A2A Client uses to listen for incoming requests:
  - Set a **PAM\_D1\_PORT** environment variable before installation. The corresponding value in the A2A Client configuration file is populated automatically.
  - Edit the `<cspmserver>daemonserver1_port</cspmserver>` parameter in the A2A Client configuration file (`/opt/Broadcom/PAM/A2A/cspmclient/config/cspm_client_config.xml`).
  - Copy a correctly configured A2A Client configuration file to the `/opt/Broadcom/PAM/A2A/cspmclient/config` directory on all A2A Client hosts after installing them from local files or a repository.
- Optionally (a default value of 28888 is preconfigured), use one of the following options to specify the port that the A2A Client uses to communicate with the PAM server:
  - Set a **PAM\_D2\_PORT** environment variable before installation. The corresponding value in the A2A Client configuration file is populated automatically.
  - Edit the `<cspmserver>daemonserver2_port</cspmserver>` parameter in the A2A Client configuration file (`/opt/Broadcom/PAM/A2A/cspmclient/config/cspm_client_config.xml`).
  - Copy a correctly configured A2A Client configuration file to the `/opt/Broadcom/PAM/A2A/cspmclient/config` directory on all A2A Client hosts after installing them from local files or a repository.
- Optionally enable IPv6:

- Set a **PAM\_ENABLE\_IPV6 [true|false]** environment variable before installation. The corresponding value in the A2A Client configuration file is populated automatically.
- To enable IPv6, edit the `<enableipv6>true</enableipv6>` parameter in the A2A Client configuration file (`/opt/Broadcom/PAM/A2A/cspmclient/config/cspm_client_config.xml`).
- Copy a correctly configured A2A Client configuration file to the `/opt/Broadcom/PAM/A2A/cspmclient/config` directory on all A2A Client hosts after installing them from local files or a repository.
- In a multisite cluster, add alternate site VIPs or node addresses to the A2A Client configuration file to configure A2A Client failover. For more information, see [Configure A2A Client Failover upon Connection Failure in a Cluster](#).
- The A2A Client is installed in the `/opt/Broadcom/PAM/A2A` directory. To see the version of the currently installed client, see the `A2A.version` file.
- Run the following command to start the A2A Client:  

```
/opt/Broadcom/PAM/A2A/cspmclient/bin/cspmclientd start
```

After the installation is complete and the client is started, the A2A Client registers with PAM.

### ***Install the A2A Client on an AIX Host***

#### **NOTE**

Before you install the A2A Client on an AIX system, ensure that your system has the correct 64-bit libidn installed. AIX only supports 64 bit. If you try to install the Client without the correct libidn, the installation stops and an error message is displayed. Also make sure to examine the User Resource Limit.

### **User Resource Limit**

The recommended data segment size for user resource limit (`ulimit -d`) is 1 GB. You have three options.

To **temporarily** increase the data segment size to 1 GB to meet OpenJDK requirements:

#### **NOTE**

If you do not make a more permanent change as shown in the following options, you must run these commands each time before you start the A2A client.

1. Before starting the A2A client, run the following command.

```
ulimit -d 1000000
```

2. Run the following command to start the A2A client (Use your real path if A2A is not installed in `/opt/catech`):

```
/opt/catech/cspmclient/bin/cspmclientd start
```

To make the data segment size change **permanent for the specified user**, modify the user setting via the AIX `chuser` command.

#### **NOTE**

The unit is represented in the number of 512-byte blocks.

```
chuser -d 2000000 root
```

To make a **system-wide change**, edit `/etc/security/limits` to increase the value.

### ***Install the A2A Client on an AIX Host***

#### **NOTE**

Before you install the A2A Client on an AIX system, ensure that your system has the correct 64-bit libidn installed. AIX only supports 64 bit. If you try to install the Client without the correct libidn, the installation stops and an error message is displayed. Also make sure to examine the User Resource Limit.

### **User Resource Limit**

The recommended data segment size for user resource limit (`ulimit -d`) is 1 GB. You have three options.

To **temporarily** increase the data segment size to 1 GB to meet OpenJDK requirements:

**NOTE**

If you do not make a more permanent change as shown in the following options, you must run these commands each time before you start the A2A client.

1. Run the following command before starting the A2A client:

```
ulimit -d 1000000
```

2. Run the following command to start the A2A client (Use your real path if A2A is not installed in /opt/catech):

```
/opt/catech/cspmclient/bin/cspmclientd start
```

To make the data segment size change **permanent for the specified user**, modify the user setting via the AIX chuser command.

**NOTE**

The unit is represented in the number of 512-byte blocks.

```
chuser -d 2000000 root
```

To make a **system-wide change**, edit **/etc/security/limits** to increase the value.

**How to Install the A2A Client on an AIX Host**

Install and configure the A2A Client on all request servers, but install only one A2A Client on a single host. Multiple Clients on the same host are not supported. If there is an existing A2A Client, uninstall it before proceeding.

**Follow these steps:**

1. Open a shell window and navigate to the location of the unzipped A2A Client installation package:

```
cd unzip_location/
```

2. Enter the following commands:

```
chmod u+x setup_aix
```

3. Start the installation script by entering the following command and options:

```
./setup_aix A2A_client_install_dir server_address [true|false]
```

Where:

- **A2A\_client\_install\_dir**: The complete pathname of the installation directory for the A2A Client software. Relative path names (that is, paths beginning with ".") are not acceptable.
- **server\_address**: One of the following options:
  - **Clustered environment**: The IP address or fully qualified domain name (FQDN) of a node at the nearest site or the site VIP if there is one. If you specify the FQDN, it must match the name in the appliance SSL certificate.
  - **Unclustered environment**: The IP address or fully qualified domain name (FQDN) of the PAM server.
- **[true/false]**: Optionally enable IPv6

**NOTE****Important Information:**

- In a clustered environment, always specify the address of the site VIP, if available. The VIP provides automatic load-balancing and failover between all the nodes at that site.
- The specified **server\_address** value is written to the A2A Client configuration file (**CSPM\_CLIENT\_HOME/cspmclient/config/cspm\_client\_config.xml**).
- In a multisite cluster, add alternate site VIPs or node addresses to the A2A Client configuration file to configure A2A Client failover. For more information, see [Configure A2A Client Failover upon Connection Failure in a Cluster](#).

4. Auto-register the A2A Client (request server) in the GUI by starting the daemon. Enter the following command:

```
A2A_client_install_dir/catech/cspmclient/bin/cspmclientd start
```

After the installation is complete and the client is started, the Client registers with PAM.



## ***Deploy an A2A Client on an AWS AMI***

### **Follow these steps:**

1. Create the instance in AWS. Do not add the device before installing the A2A Client.
2. Import the AWS AMI automatically into the appliance.  
During the import, the appliance recognizes the AWS internal IP address of the device.
3. Install the A2A Client. The A2A Client registers with the appliance using the AWS internal IP address.

### **To process credential requests, follow these steps:**

1. Activate the request server (A2A Device). This step is not required when the A2A Device has already been provisioned.
2. Associate the request script.
3. Add the authorization mapping.

## ***A2A Client Host (Request Server) Registration***

After you install the A2A Client and start it for the first time, the client sends a registration request to PAM. PAM registers the A2A Client and automatically configures an A2A device. The appliance names the device using the fully qualified domain name or the A2A Client host IP address.

To re-register the A2A Client, modify the A2A device record in the UI. Clear the **A2A** option for the **Device Type** setting. If you make change, the A2A Client responds by reregistering.

### **NOTE**

If you change the device address without changing the device name, the re-registration fails. The **Sessions**, **Logs** screen displays an error that the request server cannot register because the device name already exists.

The A2A Client is registered in an inactive state. For the A2A Client to receive credentials, activate the request server, as described in the following procedure.

## **Activate and Deactivate the A2A Request Server**

The A2A Client is registered in an inactive state. Activate the request server with the installed A2A Client.

This procedure assumes that you have:

- Installed the A2A Client software
- Started the A2A Client (CSPMClient service)

### **Follow these steps:**

1. Select **Devices**, **Manage Devices**.
2. From the Devices list, select the A2A Client and select **Update**.
3. On the **Basic Info** tab, select the **Active** option in the Request Client section
4. Select **OK** to activate the A2A Client.

To deactivate a request server, repeat the previous procedure but clear the **Active** option.

## **Uninstall the A2A Client**

This content describes how to uninstall a A2A Client on Windows and UNIX clients.

### **Uninstall an A2A Client on UNIX**

#### **Follow these steps:**

1. Stop the A2A Client:  
`$CSPM_CLIENT_HOME/cspmclient/bin/cspmclientd stop`



where `$CSPM_CLIENT_HOME` is your installation directory, for example `/opt/cloakware`

2. Run the uninstall script by entering:

```
$CSPM_CLIENT_HOME/cspmclient/bin/cspmclient_uninstall
```

This script removes all A2A Client files. However, it retains the `cloakware` directory that the installation script creates and the configuration file, if you created one during installation.

3. (Optional) If it is empty, remove the `cloakware` directory by entering the following command:

```
rmdir cloakware
```

## Uninstall an A2A Client on Windows

### Follow these steps:

1. Stop the A2A Client using one of the following steps:
  - Stop the `cspmclientd` service using the Windows Services tool.
  - Open a Command Prompt window and type the following text:
 

```
net stop cspmclientd
```
2. Use one of the following methods to launch the uninstall executable:
  - Use the Control Panel Add/Remove Programs option: Select the **PAM A2A Client** or **Password Authority Client** entry (as appropriate, depending on the version of the existing client).
  - Navigate to:
 

```
%CSPM_CLIENT_HOME%\cspmclient\Uninstall_Password_Authority,
```

 where `CSPM_CLIENT_HOME` is the A2A Client installation directory, for example, `C:\CSPM\Cloakware`. Double-click `Uninstall_Password_Authority.exe` or `Uninstall PAM A2A Client.exe` (as appropriate, depending on the version of the existing client).
 

The greeting window appears followed by the **Uninstall** window.
3. **Select Uninstall.**

When the uninstall finishes, the **Uninstall Complete** window appears. You might need to remove files manually. If so, the uninstaller identifies the files that must be manually removed.
4. Select **Done**.
5. (Optional) Remove the empty `cspm` folder.

## Target Aliases for A2A Target Accounts

A target alias enables an A2A requestor to request credentials from a specific account without transmitting the account user name and password. Target aliases are account-specific and are generated when the account is created. Privileged password accounts do not use target aliases.

The Aliases page lists aliases already created during target account set up. To add an alias, follow the instructions on the [Add Target Accounts to Target Applications](#) page.

## Start or Stop an A2A Client

You can start and stop the A2A Client from the command line or, for Windows systems, from the Windows Administrative Tools.

### Start and Stop the A2A Client on UNIX

To start the A2A client on UNIX, enter the following command:

```
cspmclientd start
```

To stop the A2A client on UNIX, enter the following command:

```
cspmclientd stop
```

## Start and Stop the A2A Client on Windows

To start the A2A client on Windows, do *one* of the following steps:

- From the **Windows Administrative Tools**, select **Component Services**. Locate and start the **cspmclientd** service. The steps for using the Windows Services Administrative tool depend on your version of Windows.
- Open a command line window and enter the following command:  

```
net start cspmclientd
```

To stop the A2A client on Windows, do *one* of the following steps:

- From the **Windows Administrative Tools**, select **Component Services** and stop the **cspmclientd** service. The steps for using the Windows Services Administrative tool depend on your version of Windows platform.
- Open a command line window and enter the following command:  

```
net stop cspmclientd
```

## A2A Client Connection Security

When an A2A Client authenticates with PAM, the PAM server identifies the client using the following data in the given order:

- Hardware fingerprint:** Uniquely identifies the client using a combination of data about the hardware characteristics of the request server. For example, CPU serial numbers and network IDs. The A2A Client generates a hardware fingerprint and passes it to the PAM server during initial registration. For subsequent client requests, the server dynamically calculates the fingerprint to validate the machine ID of the credential requestor.

### NOTE

The hardware fingerprint only changes if the hardware configuration of the request server significantly changes. When a hardware change occurs, the PAM client generates a new fingerprint. Because the fingerprint no longer matches the data on the PAM server, further client requests are refused.

To update the hardware fingerprint of an A2A Client in the PAM server, do the following steps:

- Verify that the **Enable Hardware Fingerprinting** option on the **Request Server Settings** tab on the **Settings, Credential Manager** page is enabled.
- Open the corresponding **View A2A Client** dialog and select the **Get Fingerprint** button.
- Client token:** A unique request server identifier that identifies the client in the appliance database. When an A2A Client initially registers, the server generates a unique token for the client. For subsequent client requests, the server uses the token to retrieve credentials from the database.
- Domain Name Servers (DNS):** Credential Manager uses the client host name as part of the client authentication process. Reverse IP lookup is also possible.

When a requestor application requests credentials, the credentials remain encrypted as they are transferred over the network. The A2A Client decrypts the credentials before passing them to the requestor.

## Integrity Verification

To support Integrity Verification, register the following information:

- File name
- File path
- Execution path for the client operating system and the integration method (Java, executable, DLL, or shared object)

The following table lists the details for each integration method:

Integration Method	Registered Data
Java (CSPMClient class)	<p><b>Script name:</b> The fully qualified name (including the package name) of the Java class that contains the <code>CSPMClient</code> instantiation and <code>getScriptCredentials</code> call, without the class extension.</p> <p><b>File path:</b> The absolute file path to the class file.</p> <p><b>Execution path:</b> The absolute file path to the class file. UNIX file paths cannot contain symbolic links.</p> <p><b>Example:</b> <code>com.cloakware.cspm.client.CSPMClient</code></p>
UNIX executable ( <code>cspmclient</code> , <code>cspmclient64</code> )	<p><b>Script name:</b> The name of the requestor file that contains the Credential Manager executable call.</p> <p><b>File path:</b> The absolute path to the requestor file.</p> <p><b>Execution path:</b> The absolute path from which the requestor is launched. UNIX file paths cannot contain symbolic links.</p>
UNIX shared object library ( <code>libcspmclientc.so</code> , <code>libcspmclientc64.so</code> )	<p><b>Script name:</b> The name of the requestor file that contains the shared object call.</p> <p><b>File path:</b> The absolute path to the requestor file.</p> <p><b>Execution path:</b> The absolute path from which the requestor is being launched. UNIX file paths cannot contain symbolic links.</p>
Windows executable ( <code>cspmclient.exe</code> , <code>cspmclient64.exe</code> )	<p><b>Script name:</b> The name of the requestor file that contains the executable call, including the file extension.</p> <p><b>File path:</b> The absolute path to the application file that contains the executable call.</p> <p><b>Execution path:</b> The absolute path from which the application is launched.</p>
Windows DLL	<p><b>Script name:</b> The name of the requestor file that contains the call <code>toGetCredentials</code>, including the file extension.</p> <p><b>File path:</b> The absolute path to the requestor file containing the DLL call.</p> <p><b>Execution path:</b> The absolute path from which the application is launched.</p>

The absolute file path is the complete path without symbolic links. To print the absolute file path in UNIX, use the `commandpwd-P`.

### **Refresh A2A Script Hashes**

A2A Client script hashes are used during integrity verification of A2A request scripts or applications. If you update or change an A2A request script or application, refresh the script hashes to avoid false integrity violations.

You can refresh the script hash for all the request applications on the specified request server (A2A Client).

#### **Follow these steps using the UI:**

1. Select **Credentials, Manage A2A, Clients**. The Client List page appears.
2. Select the server where the A2A client whose logs you want to view is installed and select **VIEW**. The Client Details page appears.  
When the A2A client is not reachable from the site server, you must log into the site where the A2A client is registered.
3. Select the **Get All Script Hash** button.

#### **For the CLI:**

Refresh the script hash by running the `getAllScriptHash` CLI command. For further details, see [getAllScriptHash](#).

## Add A2A Requestors

To implement A2A scripts, you add requestors in Privileged Access Manager. This procedure assumes that you have registered the request server and set it to the active status. (See [Example Requestors](#) provide registration data for the examples.

You can add scripts using the UI or the CLI:

### Add A2A Scripts using the UI

To add requestors using the UI, follow these steps:

1. Select **Credentials, Manage A2A, Scripts**.  
The Scripts list page appears.
2. Select **ADD**.  
The Add Script page appears.
3. To find an existing client, select the magnifying glass
4. Enter the **Script/App Name**, **Execution Path**, **File Path**, and script **Type**.  
**File Path** - The fully qualified path to where the executable file or script file is located.  
**Execution Path** - If the application itself is an executable file, then the Execution Path and the File Path are the same. If the application is a script, the two paths can be different.

#### NOTE

You can use standard Windows path formats, such as C:\Windows\System, or UNC (Uniform Naming Convention) paths.

5. If you use target groupings, enter descriptors for the target application.
6. Select **OK**.  
The page is updated with the registered request scripts.

To retrieve the script hash from the UI, follow these steps:

1. Select **Manage A2A, Scripts**.
2. Select the script that you want to retrieve the hash for and select **UPDATE**.  
The Script Details page appears.
3. Select **Get Script Hash**. If PAM cannot retrieve the script hash, ensure that nothing is blocking communication to the appliance. Possible causes might be the server hosting the A2A Client or a network device, such as a firewall. By default, A2A Client listens on port 28888.
4. Select **OK**.

### Add A2A Scripts Using the CLI

Use the following procedure to add requestors using the CLI.

Follow these steps:

1. Add a request server:  

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addRequestServer
RequestServer.hostName=Vienna-Lab4.cloakware.com RequestServer.ipAddress=11.2.0.4
RequestServer.active=true RequestServer.type=CLIENT Attribute.descriptor1=Vienna
Attribute.descriptor2=Lab
```
2. Enter your password at the prompt. Credential Manager returns the following XML command string.  

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
```

```

<cr.result>
<RequestServer>
<Attribute.descriptor2>Lab</Attribute.descriptor2>
<Attribute.descriptor1>Vienna</Attribute.descriptor1>
<ID>1</ID>
<createDate>Mon Nov 12 15:45:56 UTC 2007</createDate>
<updateDate>Mon Nov 12 15:45:56 UTC 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>/fvVAT2Ri4AN7zYCsweyB++/9ow=</hash>
<hostName>Vienna-Lab4.cloakware.com</hostName>
<IPAddress>11.2.0.4</IPAddress>
<type>CLIENT</type>
- 145 -Privileged Access Manager Credential Management Implementation Guide
<port>1</port>
<oldKey>
</oldKey>
<currentKey>13a3a6811160561bf8f69acf66f37f24a97b7e2b99b4afbbe61bade35c0b4108991057
a80ac4c9ecabef1d0657f14ad9911f26061bf0a4feb952e717807a72bd90663f62b2a21c35c11e4143
31a01b18594eb56c5da497ccf990f23b1855adadf294ba50e93fd25824950c4ef6115db67f61d81edb
2ebb2cbc619e2cd97786c60bd4c5e9b9a615131e8d8da7001b4b45dcaeca9be3b13a46efe5449729ad
f9399ef5b67cdfabcbcb60f7d298c151e50ec64060d5fd3c5e74652ba4198497c2933f3ef2e15600e71
74467054f2b19a26fdf5c5d1ee080b0e7d5cc269daa947e59320083de7143c6c8ff757d41a98d8caac
e690129a88e5d4e472039f8f2bc7061e7a913e070075e7dc90cdd1a248cf1ea78e5d00c9429535b502
3068472c817c36fe8a9af1bb615a6d357ace3ec30cfd1a1edf07982b95517a9066f4e0d0ce716a10f9
111943a4f9e144ba0a8f198c2a02e58df5eb0b77c7845900af8105eebc7e</currentKey>
<autoPatch>true</autoPatch>
<pendingAcknowledgement>true</pendingAcknowledgement>
<active>true</active>
<actionRequired>false</actionRequired>
<action>
</action>
<currentFingerprint>
</currentFingerprint>
<pendingFingerprint>
</pendingFingerprint>
<currentFingerprintDate>
</currentFingerprintDate>
<pendingFingerprintDate>
</pendingFingerprintDate>
<osName>
</osName>
<osVersion>
</osVersion>
<osArchitecture>
</osArchitecture>
<clientType>
</clientType>
<clientVersion>
</clientVersion>
</RequestServer>
</cr.result>
</CommandResult>

```

### 3. Add a request script:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addRequestScript
RequestServer.hostName=Vienna-Lab4.cloakware.com RequestScript.name=example.pl
RequestScript.executionPath=/opt/cloakware/cspmclient_v.3.5.0/examples RequestScript.type=Perl
RequestScript.filePath=/opt/cloakware/cspmclient_v.3.5.0/examples Attribute.descriptor1=Vienna
Attribute.descriptor=Lab
```

### 4. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<RequestScript>
<ID>1</ID>
<createDate>Mon Nov 12 15:47:35 UTC 2007</createDate>
<updateDate>Mon Nov 12 15:47:35 UTC 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>/14qoJ1SI63KgaTIKDZD8J5lWvs=</hash>
<name>example.pl</name>
<filePath>/opt/cloakware/cspmclient_v.3.5.0/examples</filePath>
<executionPath>/opt/cloakware/cspmclient_v.3.5.0/examples</executionPath>
<type>Perl</type>
<requestServerID>1</requestServerID>
<scriptHash>
</scriptHash>
</RequestScript>
</cr.result>
</CommandResult>
```

## Example Requestors

Each Privileged Access Manager A2A Client includes example applications. The examples are located in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory.

The UNIX version of the A2A Client supports symbolic links in the File Path field only.

Example	Integration Method	Registration Data
<b>Executable:</b> example.pl <b>Source file:</b> example.pl	cspmclient	<b>Script name:</b> example.pl <b>File path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Execution path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Script type:</b> Perl
<b>Executable:</b> example.ps1, example64.ps1 <b>Source file:</b> example.ps1, example64.ps1	cspmclient	<b>Script name:</b> example.ps1 <b>File path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Execution path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Script type:</b> PowerShell

<b>Executable:</b> Run_example,Example.class <b>Source file:</b> Example.java	Java	<b>Script name:</b> Example <b>File path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Execution path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Script type:</b> Java
<b>Executable:</b> example_c_interface_java <b>Source file:</b> example.c	cspmclient	<b>Script name:</b> example_c_interface_java <b>File path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Execution path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Script type:</b> C
<b>Executable:</b> example.ksh <b>Source file:</b> example.ksh	cspmclient	<b>Script name:</b> example.ksh <b>File path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Execution path:</b> \$CSPM_CLIENT_HOME / cspmclient/examples <b>Script type:</b> ksh

When entering Credential Manager request script data, you must enter the actual value for \$CSPM\_CLIENT\_HOME.

Example	Integration Method	Registration Data
<b>Executable:</b> VB_Sample <b>Source directory:</b> VB_Sample	Credential Manager MFC DLL	<b>Script name:</b> VB_Sample.exe <b>File path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VB_Sample <b>Execution path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VB_Sample <b>Script type:</b> VB
<b>Executable:</b> VC_Sample <b>Source directory:</b> VC_Sample	Credential Manager MFC DLL	<b>Script name:</b> VC_Sample.exe <b>File path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VC_Sample <b>Execution path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VC_Sample <b>Script type:</b> C
<b>Executable:</b> VBScriptSample.html <b>Source directory:</b> VB_Script_Sample	Credential Manager ATL DLL	<b>Script name:</b> VBScriptSample.html <b>File path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VB_Script_Sample <b>Execution path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\VB_Script_Sample <b>Script type:</b> VB
<b>Executable:</b> JavaScriptSample.htm <b>Source directory:</b> Java_Script_Sample	Credential Manager ATL DLL	<b>Script name:</b> JavaScriptSample.htm <b>File path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\Java_Script_Sample <b>Execution path:</b> \$CSPM_CLIENT_HOME \cspmclient\examples\Java_Script_Sample <b>Script type:</b> Java

For more information, see [Integrate A2A Applications](#).

## Configure A2A Authorization Mappings

To ensure target credential security, PAM must authorize requestors to retrieve the target credentials. Authorization mappings associate requestors and request servers with a target alias or a target group.

This topic describes how to map A2A requestors to targets and how to add an Authorization mapping.

### Mapping A2A Requestors to Targets

Before a requestor can obtain credentials for a target, you must define an A2A mapping. A mapping links requestors to targets.

You can configure authorization mappings for the following registered components:

- A requestor (script) and a target alias
- A request server and a target alias
- A request group and a target alias
- A requestor (script) and a target group
- A request server and a target group
- A request group and a target group

A mapping to a target group includes all aliases for all accounts in the group. A mapping from a request server can include all applications (scripts) on the server or you can restrict the mapping to a specific script. A mapping from a request group includes all applications (scripts) in the group.

A requestor is defined by several attributes, not all of which are necessarily used by a mapping. A mapping can use the following attributes to identify a requestor:

- **Request server (required):** The host name or IP address and associated descriptors. A mapping must specify a single request server or a request group
- **Application or script name:** The name of the program or script (for example, myProgram.exe)
- **Application or script execution path:** The path to the program on the request server
- **Application or script file path:** The path that invokes the program (for example, ./)
- **Execution user id:** The user ID that executes the program
- **Application or script hash:** A hash of the requesting program or script. This value can ensure that the program or script is not modified

A mapping must specify a request server. The other attributes are optional. If a mapping uses only a request server (or a request server group; not programs), any program on the request server can access account passwords. The program can be executed by any user. To restrict access to specific programs or users, you can configure a mapping and a script for each request server.

### ***Specifying Requestors in a Mapping***

Mappings can specify requestors as follows:

- Request group. A request group is a collection of requestors. The group identifies a collection of request servers and request scripts.
- All requesting programs on a request server
- A specific registered Request Script

Also, you can restrict each mapping to apply only when the requesting program is run as a user ID in a specific list of Execution User IDs. The mapping can specify that the execution, file path, and hash be verified. This condition implies that the requesting program has an associated registered Request Script.

### **Request Group**



If a requestor group includes a Request Server but not any Request Scripts, it implicitly includes all request programs on those request servers. If a request group specifies only request scripts, it implicitly allows them from any request server. Static request groups can only reference request servers or registered request scripts. Dynamic request groups can also reference unregistered request scripts (based on their name, file path, or execution path).

Large organizations find that dynamic request groups can scale easily.

### **All Requesting Programs on a Request Server**

A mapping can also be made to allow any requesting program on a given request server. This method does not permit any checking of the requesting program. However, as with all mappings the user ID the program is running under can be checked.

This method is useful when A2A is first deployed because it eliminates authorization as a failure reason. This feature can make it easier to develop of A2A programs.

### **Registered Request Script**

Registered Request Scripts are always associated with a specific request server. A Request Script specifies the Request Server that it runs on, its name, and an execution path.

This method gives great control but requires the creation of many mappings. This method is not as scalable as using a Request Group.

### **Request Validations**

For each mapping, request validations are done. The following table shows the scope of the validations:

Option	Scope
Request server	Validated for every application
Application name	Validated for every application
Application location	Validated only if file path is checked.
Application hash (script integrity)	Validated only if script integrity validation is checked.
Execution user ID	Validated only if execution user ID is checked.
Execution path	Validated only if execution path is checked.

### **Add an Authorization Mapping**

#### ***Prerequisite***

Before you add an authorization mapping, add the target alias or group, request server or request server group. If necessary, also add any request script for a request group mapping. If there is no verification of the script, such as integrity verification or execution path, a request script is not required.

#### ***Guidelines for Mapping Script Groups***

When you create a dynamic requestor script group, the group contains all scripts in the path that satisfy the filter criteria. The group includes scripts that are defined in the PAM database and scripts that are not.

When you map a script group that is created with filters, be aware how you set the **Check Execution Path** and **Check File Path** checkboxes:

- If you select one or both checkboxes, the authorization mapping is restricted to only those scripts that are in the database. Any scripts that are not in the database are excluded from the authorization mapping.
- If you clear the checkboxes, all scripts in the group are included in the authorization mapping.

#### ***Add a Mapping Using the UI***

**Follow these steps:**

1. Select **Credentials, Manage A2A, Mappings**.  
The Authorization Mappings page displays with a list of existing authorizations.
2. Select **ADD**.
3. For the **Target** setting, select **Group** or **Alias**.
4. Enter the target group or alias name or search for a target group or alias using the magnifying glass.
5. For the **Request** setting, select **Group** or **Client**.
6. Enter the requestor group or client name or search for an A2A requestor group or client using the magnifying glass.
7. For the **Script** setting, select whether the mapping applies to **All** applications (scripts) on the request server or an **Individual** application (script). For an individual script, enter the script name or search for the script. For A2A requestor groups, the mapping applies to all scripts.
8. Set the **Check Execution User** option.
9. Enter one or more **Execution User** IDs. Separate multiple user IDs with commas.
10. To restrict the authorization to provisioned scripts only, set one of both of the following settings:
  - **Check Execution Path**
  - **Check File Path**
11. Set the **Perform Script Integrity Validation** option. If you cannot select this validation option, no valid script hash is available. Complete the following steps:
  - a. Add the authorization mapping without selecting the validation option.
  - b. Run a query from the requestor.
  - c. Update the mapping and select this validation option.
12. Select **OK** to save the mapping.

**Add a Mapping Using the CLI****Using the CLI, follow these steps**

1. Add an authorization mapping by entering the following command:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=addAuthorization
  TargetAlias.name=ViennaAlias5 RequestServer.hostName=Vienna-Lab4.cloakware.com
  RequestScript.name=example.pl RequestScript.executionPath=/opt/cloakware/cspmclient_v.3.3.0/examples
  Authorization.checkExecutionID=true Authorization.executionUser=root Authorization.checkPath=true
  Authorization.checkScriptHash=true
```

2. Enter your password at the prompt. Credential Manager returns the following XML command string.

```
<CommandResult>
<cr.itemNumber>0</cr.itemNumber>
<cr.statusCode>400</cr.statusCode>
<cr.statusDescription>Success</cr.statusDescription>
<cr.result>
<Authorization>
<ID>1</ID>
<createDate>Mon Nov 12 15:51:06 EST 2007</createDate>
<updateDate>Mon Nov 12 15:51:06 EST 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>XOPh+2zvQDphQ0M4LPzLfyTPoiw=</hash>
<executionUser>root</executionUser>
<targetAliasID>1</targetAliasID>
<scriptID>1</scriptID>
<requestServerID>1</requestServerID>
<checkPath>false</checkPath>
```

```
<checkExecutionUser>true</checkExecutionUser>
<checkScriptHash>false</checkScriptHash>
<checkFilePath>false</checkFilePath>
</Authorization>
</cr.result>
</CommandResult>
```

## View Unsuccessful A2A Client Requests

All requests that are made to Credential Manager are stored in the Credential Manager database. You can view unsuccessful A2A client requests from the **Dashboard Overview Tab** in the **Credential Management** panel.

You can also select the **Credentials, Reports, Activities Credential Manager Activities** panel.

To view the list of the failed items on the **Credential Manager Activities** panel, select **Failed A2A Client Request In Last 30 Days**. If the **Failed A2A Client Request In Last 30 Days** item does not appear, select **Configure**, and then select the item from the configuration panel.

## Run an Example Application

This section describes running an example application on either a UNIX A2A client or a Windows A2A client.

### Run an Example Application on a UNIX Client

Follow these steps:

1. Launch the example with the target alias and the bypass cache flag set `true`. The local credential cache is bypassed and the query goes directly to the Privileged Access Manager server:

```
/opt/catech/cspmclient/examples/example.pl SydneyAlias1 true
```

#### NOTE

When using Integrity Verification in UNIX, you must use the complete path to invoke the requestor script.

2. A successful query provides the user name and password that is associated with the target alias. For example, running the Java example on a UNIX-based A2A Client yields the following result:

```
/opt/catech/cspmclient/examples/Run_example testAlias1 true
Status Code: 400
UsedId:      someaccount
Password:    q6YIbGECF0C261Xo
PASSED
```

### Run an Example Application on a Windows Client

The Windows A2A Client contains example projects that you can compile in Visual Basic, C, and C#. (Compiled programs are no longer provided.) The examples also include Java, Python, PHP, Perl, VBScript, and PowerShell scripts. The examples are in the `$CSPM_CLIENT_HOME\cspmclient\examples` folder.

#### NOTE

The PowerShell example (`example.ps1`) has an error in version 3.2. Update Line 15 to include the `-Command` parameter:

```
$output = Invoke-Expression -Command $command
```

## Modify the A2A Client Configuration File

You can edit the A2A Client configuration file for the following reasons:

- To change a configuration that is not included in the installer, such as port numbers.
- To apply a configuration change after installation, such as changing the log file location.
- To modify the log level to debug a problem.

### Modify the File

Use this procedure to modify the A2A client configuration file.

#### Follow these steps:

1. Stop the A2A Client service by entering the appropriate command:
  - **UNIX:** `cspmclientd stop`
  - **Windows:** `net stop cspmclient`
2. Navigate to the A2A client configuration file, **cspm\_client\_config.xml**. The configuration file is in one of the following directories:
  - **UNIX:** `$CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`
  - **Windows:** `%CSPM_CLIENT_HOME%\cspmclient\config\cspm_client_config.xml`
 Where `CSPM_CLIENT_HOME` is the A2A Client installation directory.
3. Edit the `cspm_client_config.xml` file in a text editor then save your changes.
4. Start the A2A Client service by entering the appropriate command:
  - **UNIX:** `cspmclientd start`
  - **Windows:** `net start cspmclient`

### A2A Client Configuration Settings

The following table describes the XML tags in the A2A Client configuration file:

XML Tag	Description
<code>&lt;applicationtype&gt;</code>	Valid values are <code>cspm</code> or <code>cspm_agent</code> . Default: <code>cspm</code>
<code>&lt;cacheallow&gt;</code>	Enables or disables credential caching on the A2A Client. Default: <code>true</code> .  This setting overrides the PAM <code>cacheBehavior</code> setting. If the <code>&lt;cacheallow&gt;</code> tag is <code>true</code> , then the Client follows the <code>cacheBehavior</code> setting. If the <code>&lt;cacheallow&gt;</code> tag is <code>false</code> , then the <code>cacheBehavior</code> setting is ignored.
<code>&lt;loglevel&gt;</code>	Specifies the log level. The following entries are valid levels (in descending order): <ul style="list-style-type: none"> <li>• OFF</li> <li>• SEVERE</li> <li>• WARNING</li> <li>• INFO</li> <li>• CONFIG</li> <li>• FINE</li> <li>• FINER</li> <li>• FINEST</li> <li>• ALL</li> </ul> The default level is OFF. Entry is case insensitive.

<cspmserver>	Specifies the host name of the PAM appliance. The installer sets this value.
<cspmserver_port>	The default port on which the appliance listens. The default is blank. For HTTPS, the default is 443. If the server port is changed from 443, you must modify this value.
<daemonserver1_port>	The A2A Client uses this port to listen for local requests from client stubs. The daemon validates that the request is local. The default value is 28088.
<daemonserver2_port>	Identifies the port that the A2A Client listens for local requests from PAM. Default port: 28888 If the value is 1, the A2A client does not listen for external requests. Instead, the A2A client polls the appliance for event information.
<eventpolling_interval>	(Optional) Specifies the interval, in seconds, after which the A2A Client polls the appliance for events. If no value is specified, the Client uses the default polling interval of 120 seconds.
<logfile>	Specifies the location of the log file that is used by the A2A Client. The installer sets this value.
<c_logfile>	The log file that is used by the service and stateless client interface stubs. <ul style="list-style-type: none"> <li>Windows default: C:\WINDOWS\TEMP\cspm_c_client_log.txt</li> <li>UNIX/LINUX default: /tmp/cspm_c_client_log.txt</li> </ul> All users of the A2A Client must have write access to the log file directory. The c_loglevel setting controls the detail in the log file. The syntax is case-sensitive: <c_loglevel>LEVEL</c_loglevel> LEVEL is one of the following values, in descending order: <ul style="list-style-type: none"> <li>OFF</li> <li>SEVERE</li> <li>WARNING</li> <li>INFO</li> <li>CONFIG</li> <li>FINE</li> <li>FINER</li> <li>FINEST</li> <li>ALL</li> </ul> The default level is OFF.
<patch>	Specifies patch management attributes, as in the following XML tags: frequency, starthour, and endhour.
<frequency>	Specifies the frequency at which the A2A Client polls the appliance for an update. Valid values are daily or weekly. The default value is daily.
<startHour>	Determines the interval at which the A2A Client randomly polls the appliance for a version check. Valid values are 0 -23. The default value is 0 (12 A.M.).
<endHour>	Determines the interval by which the A2A Client randomly polls the appliance for a version check. Valid values are 0 -23. The default value is 5 (5 A.M.).
<operation>	For internal use only.

<preserveCacheBetweenRestarts>	Enables caching to local storage. before release 3.0.1, A2A Clients maintained the credential cache in memory <i>and</i> on local storage by default. Beginning with release 3.0.1, the default behavior is to maintain the cache <i>only</i> in memory. To enable local storage, set the <preserveCacheBetweenRestarts> tag to true . Caching credentials locally reduces network traffic and increases reliability. The A2A Client can use the cached credentials instead of accessing PAM to process the credential requests. The A2A Client, like the appliance, provides credentials only in response to authorized credential requests. When a password change for a target account is triggered, the appliance notifies any A2A Client that is caching the password. This notification ensures that A2A Clients do not cache target passwords that are out of date.
<c_connection_timeout>	Indicates the value of connection timeout (in seconds) from A2A Client to A2A Daemon
<c_read_timeout>	Indicates the value of read timeout (in seconds) from A2A Client to A2A Daemon.
<cspmserver_connection_timeout>	Indicates the value of connection timeout (in seconds) from A2A Daemon to the PAM Server.
<cspmserver_read_timeout>	Indicates the value of read timeout (in seconds) from A2A Daemon to the PAM Server.

## How the A2A Client Configures Cache Credentials to Local Storage

To reduce network traffic and increase reliability, the A2A Client locally caches credentials as specified in the target account details. When target credentials are cached, the A2A Client does not need to access Privileged Access Manager to process the target credentials request. The A2A Client uses the same application logic as Privileged Access Manager to ensure that it provides credentials only in response to authorized credential requests.

When a user or a scheduled update triggers a change of target account passwords, Credential Manager sends notification of the change to any A2A Client that might be caching the password. This process ensures that A2A Clients do not cache target passwords that are out of date.

## View A2A Client Logs

You can view A2A Client logs with the GUI, so you can troubleshoot client issues. This feature is not available for clients with event polling enabled.

### Follow these steps:

1. Select **Credentials, Manage A2A, Clients**. The Client List page appears.
2. Select the server where the A2A client whose logs you want to view is installed and select **VIEW**. The Client Details page appears.  
When the A2A client is not reachable from the site server, you must log into the site where the A2A client is registered.
3. Select the **Get Logs** button. A zip file containing the Tomcat logs directory is downloaded to your browser. The default maximum file size is 20 MB. You can configure the maximum file size using the `getLogsMaxSize` {SystemProperty.SYSTEM\_PROPERTY\_MAX\_LOG\_SIZE} property setting. For further details, see the description of the `setSystemProperty` CLI command.

## Update an A2A Client Key

The A2A Client key is used to encrypt communication between the A2A Client and the Privileged Access Manager appliance. As an added layer of security, you can update the A2A Client key regularly to mitigate possible detection and misuse of the key.

### Follow these steps:

1. Select **Credentials, Manage A2A, Clients**. The Client List page appears.

2. Select the server where the A2A client whose logs you want to view is installed and select **VIEW**. The Client Details page appears.  
When the A2A client is not reachable from the site server, you must log into the site where the A2A client is registered.
3. Select the **Change Key** button.

## View A2A Client Status and Troubleshoot Connection Issues in a Cluster

This content describes how to view the status of the connection between PAM and an A2A Client and troubleshoot issues with that connection. The content also describes how to generate a hardware fingerprint for the request server.

### Verify A2A Client Connection Status

Use the following procedure to verify the status of the connection between an A2A Client and the PAM node or PAM site (represented by a VIP) with which it is registered.

#### Follow these steps:

1. Log into the PAM UI on the PAM server on which the A2A Client was originally registered (the *owning* PAM server).
2. Select **Credentials, Manage A2A, Clients**. The **Client List** page opens.
3. Select the request server where the A2A Client whose status that you want to view is installed and select **VIEW**.  
The **View A2A Client** dialog opens.

#### NOTE

The name and address of the PAM node with which the A2A Client is registered are indicated by the **Owning PAM Member** and **Owning PAM Member Address** fields.

In a multisite cluster, the name and address of the VIP of the site with which the A2A Client is registered are indicated by the **Owning PAM Site** and **Owning PAM Site Address** fields.

The **Connection Status** field displays an icon that indicates the status and time of the last connection attempt from PAM to the A2A Client. The following table provides details about the connection status values that are indicated by the colored status icon.

Icon Color	Status	Condition
Green	Online	The owning PAM node or other member of the same site has successfully connected to the A2A Client within the configured threshold.
Orange	Unknown	The state of the A2A Client is unknown. The owning PAM node or no PAM nodes in an owning site were unable to connect to that client within the configured threshold. Event processing for that client is therefore stopped.
Red	Offline	The A2A Client service <code>cspmcliclientd</code> is stopped.

4. To refresh the information in the **Connection Status** field to provide updated data, select the **Check Connection Status** button.

If the **Connection Status** field still shows orange, the status of the A2A Client is unknown because neither the owning PAM node nor any PAM nodes in an owning site can connect to it.

Event processing for this A2A Client is therefore stopped on all PAM nodes and the A2A Client cannot receive event notifications or obtain user credentials. To resolve this issue, see [Troubleshoot Outbound A2A Client Connections](#) and [Troubleshoot Inbound A2A Client Connections](#) later in this topic.

### Troubleshoot Outbound A2A Client Connections

Use this procedure to attempt to establish an *outbound connection* from a node at another site in the cluster to allow PAM to send event notifications.

**NOTE**

This procedure does *not* reestablish an *inbound* connection from the A2A Client connection, which is required to obtain user credentials. For more information, see *Troubleshoot Inbound A2A Client Connections* later in this topic.

**Follow these steps:**

1. Log into the UI of a PAM node at any other site in the cluster and navigate to one of the following locations:
  - On a primary node: **Credentials, Manage A2A, Clients**
  - On a secondary node: **Credentials, A2A Clients**
2. Select the problem request server (identified by the orange bubble in the **Connection Status** field) from the list and select the **View** button. The **View A2A Client** dialog opens.
3. Select the **Check Connection Status** button. If any operational node in the cluster has a clear network path to the A2A Client, the **Connection Status** field should now be green.
4. If the **Connection Status** field is still orange, no node in the cluster has a clear network path to the A2A Client. Do the following operations in order to attempt to restore outbound connectivity:
  - a. Check that the A2A Client (cspmclientd) process is still running on the request server.
  - b. Restore operation of the owning member or site.
  - c. Reconfigure your network to provide a clear network path to the A2A Client from another node or site.

**Troubleshoot Inbound A2A Client Connections**

The A2A Client requires an *inbound* connection to obtain credential information. By default, such a connection can only be established with the owning node or a member of the owning site. To reestablish credential processing, do one of the following operations:

- Restore operation of the owning member or site.
- Temporarily register the A2A Client with another site.
- [Configure A2A Client failover](#) by adding the addresses of alternate PAM nodes or VIPs in the cluster to the A2A Client configuration. If a connection to the first defined location fails, the A2A Client attempts to connect to the next defined location, and so on.

**Generate a Hardware Fingerprint for the Request Server**

If [hardware fingerprinting is enabled](#), Credential Manager can use generated hardware fingerprints to uniquely identify request servers. Hardware fingerprints combine hardware characteristics of the request server, such as CPU serial numbers and network IDs.

To generate a hardware fingerprint for a request server, select the **Get Fingerprint** button.

**NOTE**

The **Get Fingerprint** button only appears if hardware fingerprinting is enabled.

To see the date and time that the current hardware fingerprint was generated, select the **Fingerprint** tab.

**Configure an A2A Client to Use Another Server**

If you have previously used your A2A Client installation for one server and are now pointing it to a different server, delete the following cache file before starting the A2A Client daemon or service again:

```
$CSPM_CLIENT_HOME/cspmclient/config/data/.cspmclient.dat
```

where `$CSPM_CLIENT_HOME` is the location and name of your installation directory. Example: `/opt/cloakware`.

Use the following procedure to reconfigure an A2A Client to use a different Privileged Access Manager appliance.



**Follow these steps:**

1. Stop the A2A Client. See [Stop the A2A Client](#).
2. Navigate to `$CSPM_CLIENT_HOME/cspmclient/config/data/`.
3. Delete the `.cspmclient.dat` file.
4. Update the `<cspmserver>` entry in the A2A Client configuration with your new server name. Example:  
`<cspmserver>new_server.company.com</cspmserver>`  
 The configuration file is located at `$CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`.
5. Restart the A2A Client. See [Start the A2A Client](#).

## Configure A2A Client Failover in a Multisite Cluster

*A2A Client failover* enables A2A Clients in a multisite cluster to connect to nodes at other sites if their current connection has failed.

**NOTE**

A2A Client failover was previously known as the *multi-home* feature.

To enable A2A Client failover, add the addresses of one or more alternate PAM nodes or site VIPs to the A2A Client configuration file. When a connection to the owning node or site fails, the A2A Client attempts to connect to the other specified addresses in sequential order. If no attempts are successful, an error code is returned.

**Follow these steps:**

1. Open the A2A Client configuration file in a text editor:  
`$CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`  
 where `$CSPM_CLIENT_HOME` is your installation directory, for example, `/opt/cloakware`.
2. Add `cspmserver` and `cspmserver_port` XML entry pairs for each alternate node or site *below* the existing entry pair, which defines the original node or VIP specified during installation.  
 The following example includes three `cspmserver/cspmserver_port` entry pairs. The first pair represents the original PAM node or site VIP. The second two pairs specify the alternate nodes or site VIPs. The order of the entries in the file determines the connection order.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <applicationtype>cspm</applicationtype>
  <cacheallow>true</cacheallow>
  <loglevel>WARNING</loglevel>
  <cspmserver>cspm1.cloakware.com</cspmserver>
  <cspmserver_port></cspmserver_port>
  <cspmserver>cspm2.cloakware.com</cspmserver>
  <cspmserver_port></cspmserver_port>
  <cspmserver>cspm3.cloakware.com</cspmserver>
  <cspmserver_port>80</cspmserver_port>
  <daemonserver1_port>27088</daemonserver1_port>
  <daemonserver2_port>28888</daemonserver2_port>
  <logfile>C:\cspm\cloakware\cspmclient\log\cspm_client_log.txt</logfile>
  <c_logfile>C:\WINDOWS\Temp\cspm_c_client_log.txt</c_logfile>
  <patch>
    <frequency>daily</frequency>
    <starthour>0</starthour>
    <endhour>5</endhour>
  </patch>
  <operation>production</operation>
</configuration>
```

3. Save your changes.

## Configure A2A Client Event Polling

If you disable event listening for an A2A Client, you must configure the Client to poll PAM for event messages. Event information includes messages, such as **get script hash** or **get fingerprint**.

When you enable event polling, the A2A Client contacts and queries the PAM server for event data at a regular polling interval. The PAM server places the events in a queue, and they remain in the queue until the A2A Client sends a request to retrieve event data.

### WARNING

Enabling event polling increases network traffic between the appliance and A2A Client. If too many A2A Clients run event polling, it impacts performance at the appliance.

### Prerequisite Steps for A2A Clients Previously Configured to Listen for Events

If the A2A Client is already registered with PAM as device of type **A2A** on the **Devices** screen (as shown in the following screen capture), do this procedure before registering that client as a polling device.

#### Follow these steps:

1. Open the PAM UI on the PAM server with which the A2A Client is registered.
2. Navigate to **Devices, Manage Devices**.
3. On the **Devices** screen that opens, select the request server from the list and select the **Update** Button. The **Update Device** dialog opens, showing how the A2A Client is configured in the **Device Type** section as shown in the following screen capture:

The screenshot shows the 'Update Device' dialog box. Under the 'Device Type' heading, there are three radio button options: 'Access', 'Password Management', and 'A2A'. The 'A2A' option is selected. Below these options is the text 'Request Client'. There are two text input fields labeled 'Description 1:' and 'Description 2:'. The 'Description 1' field contains the text 'A2A Client'. At the bottom of the dialog, there are two checkboxes: 'Active:' which is checked, and 'Preserve Hostname:' which is unchecked.

4. Do one of the following steps depending on the **Device Type** selection:
  - If either or both of the **Access** and **Password Management** options are set, unset the **A2A** option and select the **OK** button.
  - If only the **A2A** option is set, do the following steps:
    - a. Select the **Cancel** button to exit the **Update Device** screen.
    - b. Back on the **Devices** screen, select the **Delete** button to remove the existing device entry.

## Enable Event Polling

To enable event polling, modify the A2A Client configuration file.

### Follow these steps:

1. Open the A2A Client configuration file in a text edit. The file is in the directory:  
`$CSPM_CLIENT_HOME/cspmclient/config/cspm_client_config.xml`  
where `$CSPM_CLIENT_HOME` is the installation directory, for example, `/opt/cloakware`.
2. Set the external listening port (`daemonserver2_port`) to 1, as shown:  
`<daemonserver2_port>1</daemonserver2_port>`
3. Optionally, change the default polling interval of 120 seconds. For example, change it to 180 seconds:  
`<eventpolling_interval>180</eventpolling_interval>`
4. Save your changes.

---

# Implementing Secrets Management

---

The topics in this section provide end-to-end instructions for configuring Secrets Managements. See [Secrets Management Overview](#) for details about Secrets Management.

- [About Secrets Management and Roles](#)
- [Administering Users, Vaults, and Secrets](#)
- [Configuring Secrets Authorization](#)

## About Secrets Management and Roles

PAM includes specific roles and privileges that are specific to secrets management.

PAM provides granular permissions over vaults and secrets. These granular permissions let administrators securely provide the appropriate access to authorized users. For example, some users should only be able to view or use secrets (access). Others may be able to manage secrets and assign vaults (administration).

- **Secret Viewer:** Can view secrets. Secret Viewers can be assigned to one or more vaults.
- **Secret Owner:** Can manage (create, update, and delete) secrets. Secret Owners can be assigned to one or more vaults.
- **Vault Owner:** In addition to Secret Owner capabilities, Vault Owners can manage vaults. They can assign Secret Owners or other Vault Owners and can delete the vaults.
- **Vault Administrator:** In addition to Vault Owner capabilities, Vault Administrators can create vaults and can assign the initial users as Secret Owners or Vault Owners.

Secret Viewers, Secret Owners, and Vault Owners are scoped, meaning that these users only see the vaults to which they are assigned and the secrets that are stored within those vaults. The Vault Administrator role is not scoped, so it has visibility across all vaults.

Users assigned to a vault as a Secret Viewer, Secret Owner, or Vault Owner have access to view all secret values stored in the vault (and manage them, if assigned an owner role). If shared access is undesirable or if a narrower scope is required, you should separate the secrets into separate vaults.

In addition, Global Administrators and Delegated Administrators have all required privileges by default. Global Administrators and Delegated Administrators can perform secret management tasks with full Vault Administrator privileges.

### **Considerations for Secrets Management and Roles**

One of the goals of Secrets Management is to retain governance and oversight with a Security Team, while distributing management and day-to-day maintenance to others within the user community. This segregation of duty model enables oversight, while still allowing select users the necessary control to add and manage their own secret content.

When assigning roles to key users, consider the level of granularity and least-control principles that each user requires to perform their required tasks. Assign those users enough control to complete those tasks, but no more than is required. Base your decision on how to assign roles on your organizational needs, your users, and the tasks that they perform. This decision has no right or wrong answer.

For example, when assigning the Vault Administrator role, consider the following items:

- Who in the organization should control how and when Vaults are created and initially assigned?
- Should this Vault Administrator be a single person, a select few throughout the organization, or maybe some or all of the members of the Security Team?

Another way to determine which roles to assign to users is to consider the “span of control”. This consideration also has implications for vault and secret management, and for role management. For example, vaults contain a collection of secrets. Vault Owners are able to view and manage all of the secrets within the vaults that are assigned to them. Assigning the Vault Owner role to someone for vaults that encompass a large division or organization can over-expose information among the Vault Owners.

Similarly, Secret Viewers are able to view the secrets within the vaults that are assigned to them. Secret Owners are able to view and manage the secrets within the vaults that are assigned to them. Assigning the Secrets Viewer or Secrets Owner role to users for secrets that encompass a large division or organization can over-expose information to these users.

#### NOTE

If there are two Secret Viewers or Secret Owners that are assigned to a vault, they can see (and Secret Owners can manage) the secrets of each other. If this shared access is undesirable, assign one vault per user.

Creating vaults and assigning Vault Owners (or secrets and Secret Viewers or Secret Owners) that are narrowly focused gives cleaner data segregation. However, this initial configuration requires more effort to set up. Symantec recommends that you consider starting with a small span of control, such as a product or application team that must manage secrets. Assign the Secret Viewer or Secret Owner role to a single manager or devops person and assign the Vault Owner role to another individual, as appropriate. Ultimately, you decide the balance between the level of security and the ease of convenience. Again, there is no right or wrong answer to this decision.

### Assigning Users the Secrets Management Role and Granular Roles

Before you can assign the Secret Viewer, Secret Owner, Vault Owner, or Vault Administrator role to users or user groups, you must first assign the *Secrets Management* role. The Secrets Management role provides the user or user group access to the Secrets Management functionality. A user or user group can only be assigned to a vault after they have been assigned this role.

Note: The Secrets Management role lets users and user groups access the Secrets menu in PAM. However, they are unable to see or manage any vaults or secrets until they are assigned a Vault Owner, Secrets Owner, or a Secret Viewer role for a vault.

A Global Administrator or Designated Administrator can assign the initial Secrets Management role.

You assign the Secrets Management role from the User or User Group details window.

1. Select the Roles tab.
2. Click the plus (+) icon.
3. Select the **Secrets Management** entry and add it.
4. After selecting the role on this tab, a User Group row appears on the list. Click the plus (+) icon in this row, click the pencil icon, and then select **All Users**.

See [Configure Users](#) for procedures on adding and updating users.

After assigning the Secrets Management role to a user or user group, that user can log in and will see the Secrets PAM menu option. Assign the users more granular roles:

- To assign the Vault Administrator role:
  - a. In the User or User Group edit page, click on the **Credential Manager Groups** tab.
  - b. Select the Vault Administrator entry on the left side under Available Groups.
  - c. Click the arrow to move the administrator to the right side.
- To assign the Secret Viewer, Secret Owner, or Vault Owner roles:
  - a. When creating or editing a vault, select the **Vault Managers** tab
  - b. Select a Secrets Management user on the left side.
  - c. Click the arrow to move the user to the right side.
  - d. Select **Secret Viewer**, **Secret Owner**, or **Vault Owner** for this user in the drop-down menu.

See [Managing Vaults](#) for procedures on adding or updating a Vault.

Global Administrators and Delegated Administrators have all required roles by default.

## Administering Users, Vaults, and Secrets

Once you have assigned your initial roles and provided access to the Secrets Management functionality, you can begin creating and managing vaults and secrets using the appropriate procedures. See [About Secrets Management and Roles](#) for procedures on assigning roles.

- [Managing Vaults](#)
- [Managing Secrets](#)
- [Managing Secret Types](#)

You can also perform many of these operations using the PAM API or a command line interface (CLI):

- For information on using the PAM API to perform these operations, see [PAM External REST API](#).
- For information on using the Remote CLI to perform these operations, see [Remote CLI and Credential Manager Java API](#).

## Managing Vaults

This section describes how to add, update, delete, and import or export Vaults.

### Adding or Updating a Vault

To add or update a Vault:

1. As a Global Administrator or Vault Administrator, select **Secrets, Manage Vaults**.
2. On the Vaults page:
  - To add a new Vault, click **Add**. The Add Vault modal appears
  - To update an existing Vault, select the Vault from the list to be updated and click **Update**. The Update Vault modal window appears

The resulting modal window has a few tabs:

- On the Vault Info tab, enter a Name and Description to identify this vault and click **OK**. The vault name must be unique.
- On the Vault Managers tab, set the users or groups that have access to this vault:

#### **TIP**

Adding a user group to a vault gives all of the users in that group the same access to the vault, as defined by the role assigned to the group.

- a. Add or remove individual users or user groups by dragging them to the appropriate column.
  - b. Add or remove multiple users or user groups by selecting them and using the arrows to move them to the appropriate column.
  - c. Once added to the right side, set the Secret Roles for the user or user group for this vault and click **OK**. See [About Secrets Management and Roles](#) for details about the available roles.
- On the Secrets tab, add, copy, update, or delete the secrets for this vault and click **OK**. Go to System Info, Licenses to see the number of secrets used.

#### **NOTE**

You can also add a secret to an existing vault without editing any other information about the vault. See [Managing Secrets](#).

## **Deleting a Vault**

Deleting a Vault removes it permanently from PAM. You can only delete an empty vault. You must delete all secrets from a vault before you can delete it.

You cannot restore a deleted Vault. However, deleting the vault does not delete the users or user groups that are assigned to them.

As Global Administrator or Vault Administrator, to delete a Vault:

1. Select **Secrets, Manage Vaults**.
2. Select the Vault to update and click **Delete**.
3. When prompted to confirm the action, click **Yes** to delete the Vault.

## **Importing and Exporting Vaults**

Vault Administrators can export and import vaults in PAM. For example, you might import a vault as an alternative to manually or programmatically creating a vault. You import vaults using a CSV file.

You can also export all current vaults. All vaults and vault details (users, user groups, and a list of secrets) are exported to a CSV file. The secrets contained in the vault are not exported.

To import a vault:

1. Select **Secrets, Manage Vaults**.
2. Click **Import**. The Import/Export Vaults modal appears.
3. Click **Choose file** to navigate to a CSV file containing the vault information to import (or type the file location directly into the **File** field).
4. Click **Import Vaults**.

To export a vault:

1. Select **Secrets, Manage Vaults**.
2. Click **Export**. PAM generates a CSV file containing the information for all existing vaults.

### ***Vault CSV file format***

The file that contains vault information must be a CSV file containing the following information for each vault. The first line must be a header containing Type,Vault Name,Description,Users,User Roles,User Groups,User Group Roles.

- Type: Always *Vault*.
- Vault Name: A unique name for the vault.
- Description: A description of the vault.
- Users: The users that have access to this vault. Separate multiple users with the vertical bar symbol (|).
- User Roles: The Secrets Management role that is assigned to the corresponding user in the Users column. Each user in the User column must be assigned a Secrets Management role. If multiple users are listed in the User column, separate User Roles with the vertical bar symbol (|).
- User Groups: The user groups that have access to this vault. Separate multiple user groups with the vertical bar symbol (|).
- User Group Roles: The Secrets Management role that is assigned to the corresponding user group in the User Groups column. Each user group in the User Group column must be assigned a Secrets Management role. If multiple user groups are listed in the User Groups column, separate User Group Roles with the vertical bar symbol (|).

All fields are required except for the Description field. You must include either the Users and User Roles fields or the User Groups and User Group Roles fields, or both.

From the Import/Export Vaults modal, click Download Sample File to see an example of a valid vault CSV file. You can download this file, edit it, and use it to import your vaults.

## Managing Secrets

A secret can be any type of information that your organization regards as secret and proprietary, and to which you want to control access. For example, a secret might be an SSL certificate, database credential in a configuration file, a JSON object, an API, or a password for user access.

Secrets are stored using a plain-text format, such as JSON, XML, or TXT. Binary formats are not supported.

This section describes how to view, copy, add, update, and delete secrets. It also describes how to manage Secret Types and Secret Formats. This section is designed for secret administrators (users with the Vault Administrator, Vault Owner, Secret Owners, or Global Administrator or Designated Administrator roles).

Secret consumers (users or processes that require secrets to perform tasks) can obtain access to secrets through the PAM Access Policy or through the A2A Mapping Policy.

### NOTE

By default, secret administrators do not have an ability to view nor manage PAM Access Policies nor A2A Mapping used for authorization.

### Adding or Updating a Secret

When adding or updating a secret, you select the vault information, assign Secret Types, and define any future actions.

To add or update a secret:

1. Select **Secrets, Manage Vaults**.
2. Select the vault to update and click **Add Secret**.
3. You can manually add or update a secret or you can upload a file containing the secret:
  - To upload a secret, click **Upload Secret** and browse to the file that contains the secret. The secret file must be a text-based file (such as a .txt, .json, or .xml file) up to a maximum of 8,000,000 characters.
  - To manually add or update your secret, enter the following information:
    - Secret Name: Set a unique name to identify this secret.
    - Aliases: Enter how the entity using the secret is identified in the authentication source (for example, username or client ID).
    - Secret Type: Select the type of secret from the drop-down list. The Secret Type must exist before you can add it to a vault. See [Managing Secret Types](#).
    - Secret Format (optional): Once a Secret Type is selected, all available formats display. Select a Secret Format and click **Insert Format** to populate the secret value with the selected format.
    - Descriptor 1 and Descriptor 2 (optional): PAM can use the descriptor fields to identify the secret. Descriptors are also by dynamic rules, which is useful when granting programmatic access using an A2A client.
    - Future Actions: Select what actions should apply to the secret and the time that the action should occur. Time is based on GMT:
      - Expire Secret: The secret expires after the date and time set, and users can no longer use them. However, expiring a secret does not remove it from the system. Enter the time in the format HH:MM:SS.
      - Delete Secret: PAM deletes the secret at the date and time set. Note that you cannot restore a deleted secret. Select a time for deletion from the drop-down menu (PAM only deletes secrets at the top of the hour).

### NOTE

If a secret is expired or deleted, then no user nor process can access it. PAM treats these secrets as if they do not exist.

4. Click **OK**.



## **Deleting a secret**

Deleting a secret removes it permanently from the vault and from PAM. You can neither restore nor recover a deleted secret.

To delete a secret:

1. Select **Secrets, Manage Secrets**.
2. Select the secret to delete and click **Delete**.
3. When prompted to confirm the action, click **Yes**. PAM deletes the secret at the top of the hour.

## **Viewing or Copying a Secret**

To view a secret or copy a secret into your clipboard as a Vault Administrator, Vault Owner or Secrets Owner:

1. Select **Secrets, Manage Secrets**.
2. Select the secret to view or copy and click **View**. The View Secret modal appears. The secret is obscured in this view. Click the eye icon to view the unobscured secret value.

From this modal, you can:

- Copy the secret value into your clipboard by clicking the clipboard icon.
- View the secret by clicking the pencil icon.

## **Automatically Expiring or Deleting a Secret**

When you add or update a secret you have the option to make it expire or be deleted after a specified number of days. An expired secret is not removed from PAM, but a user or a client can no longer access the secret. A deleted secret is removed from PAM. In both cases, PAM treats these secrets as if they do not exist. No user nor process can access it. However, you can manually extend the secret expiration or deletion date after it is set. You can also set the maximum number of days that can be specified before the secret is expired or deleted. Additionally, you can configure the timing and the content of the email that PAM sends to the secret owner when a secret is about to expire or be deleted.

### ***Extending the Expiration or Deletion Date***

Complete the following steps to manually extend the expiration or deletion date of a secret. The secret must be set to expire or be deleted and be eligible for extension.

1. Select **Secrets, Manage Secrets**.
2. Select the secret or secrets to extend and click **Extend**.
3. In the Extension (Days) box, set the number of days to extend the secret expiration.
4. Click **Yes**.

### ***Setting the Maximum Numbers of Days to Set for Expiration or Deletion***

By default, the maximum number of days that you can specify before a secret is expired or deleted is 365. You can configure the maximum number of days in PAM.

To set the maximum number of days that you can specify before a secret is expired or deleted:

1. As a PAM administrator with the appropriate privileges, select **Global Settings, Secrets Management**.
2. Under Maximum Secret Extension (Days), set the maximum number of days that can be specified before the secret is expired or deleted, up to 365 days.
3. Click **Ok** to confirm the setting.

### ***Configure the Expiration and Deletion Notification***

By default, PAM notifies the secret owners that their secrets are expiring or are being deleted seven days before the event. You can modify the content of the notification email and the number of days before the event that PAM sends the notification email.

To modify the secret expiration or deletion notification email:

1. As a PAM administrator with the appropriate privileges, select **Settings, Credential Manager**.
2. Click the Email Templates tab.
3. For the Notify of Upcoming Secret Expirations email template, configure the following settings:
  - Secret Expiration (Days): Set how many days before the event that this email notification is sent.
  - Secret Expiration Subject: Enter the text to display in the subject line of the notification email.
  - Secret Expiration Body: Enter the text to display in the body of the notification email.
  - Click **Ok** to confirm the setting.

## Managing Secret Types

A secret type is a way to categorize and label different types of secrets, such as tokens, certificates, or db connection strings. PAM administrators have the ability to build this list as they see fit for their organization. Only Global Administrators and Vault Administrators can manage secret types. Vault owners and secret owners cannot edit secret types.

Optionally, you can give a secret type one or more different secret formats (or templates) for further clarity. Think of the secret format as a hint that is provided to someone adding this secret type. To make secret creation easier, you can apply an existing secret format or create custom formats.

PAM also lets you upload an example payload.

### NOTE

PAM does not do any kind of format validation or checking on the information supplied. A secret value is a plain text field.

Some examples of secret types and secret formats include (but are not limited to):

Secret Type	Possible Secret Formats
Token	JWT, OAuth, Access, HomeGrown
DB Connection	JDBC, ODBC
KubeConfig	Kube v1.22, Kube v1.23

PAM provides editable samples for some of these secret types and formats that you can use, modify, add to or delete, as needed.

### Adding a Secret Type

To add a secret type:

1. Select **Secrets, Manage Secret Types**.
2. Click **Add**. The Add Secret Type modal appears.
3. Enter a unique name to identify the secret type and click **Add**.
4. Manually add a secret format or upload a file containing the expected structure, format, or contents.
 

Note: PAM does not validate the secrets against the Secret Format. Secret Formats do not need to match the expected format

  - To upload a secret format, click **Upload Format** and browse to the file that contains the secret format. The secret format file must be a valid .txt, .json, or .xml file, up to a maximum of 2048 characters.
  - To manually add a secret format:
    - Enter a unique name to identify the Secret Format
    - Enter the secret format. The secret format can be up to 2048 characters.
5. Click **OK**.

## **Updating a Secret Type**

You can update the secret format associated with a secret type.

To update a secret type:

1. Select **Secrets, Manage Secret Types**.
2. Select the secret type for the format that you want to update and click **Update**. The Update Secret Type modal appears.
3. Select the format type that you want to update and click **Update**.
4. Manually update the secret format or upload a file containing the secret format:
  - To upload a secret format, click **Upload Format** and browse to the file that contains the secret format. The secret format file must be a valid .txt, .json, or .xml file, up to a maximum of 2048 characters.
  - To manually update a secret format:
    - Enter a unique name to identify the secret format.
    - Enter the secret format. The secret format can be up to 2048 characters.
5. Click **OK**.

## **Deleting a Secret Type**

Deleting a secret type removes it and its associated Secret Format permanently from PAM. You cannot restore a deleted Secret Type.

Note: You cannot delete a secret type if it is actively in use by a secret. You also cannot delete the Generic Secret Type.

To delete a secret type:

1. Select **Secrets, Manage Secret Types**.
2. Select the secret type that you want to delete and click **Delete**. The Update Secret Type modal appears.
3. When prompted to confirm the action, click **Yes**.

## **Copying a Secret Format**

To copy a secret format into your clipboard:

1. Select **Secrets, Manage Secret Types**.
2. Select the secret type for the format that you want to copy and click **Update**. The Update Secret Type modal appears.
3. Select the format type that you wish to copy and click **Copy**.
4. Modify the data as required and click **OK** to save this as a new format type.

# **Configuring Secrets Authorization**

Secret administrators (Vault Administrators, Vault Owners, and Secret Owners) are responsible for creating and managing vaults and secrets in PAM. However, secret consumers (users, user groups, and processes) also need access to these secrets to perform day-to-day or automated tasks, without being able to change or delete them. Also, secret consumers should be able to see only those secrets to which they are authorized to see.

PAM allows for authorized access through multiple sources:

- PAM Client (Desktop)
- PAM Agent (Windows Desktop)
- A2A Agent (Programmatic Access)

## Managing Secret Authorizations (Mappings)

In PAM, authorizations are required as an additional layer of control to allow a specific A2A Agent running on a specific Request Server to request a specific secret. These authorizations are referred to as *mappings*.

Mappings are a type of authorization policy that apply to the programmatic access use cases.

There are two types of mappings:

- Credential mappings authorize Request Servers to access traditional credentials.
- Secret mappings authorize a Request Server or Request Group (a group of Request Servers) to access a secret or secret group.

This section describes secret mappings. See [Configure A2A Authorization Mappings](#) for information on credential mapping.

Before you add a secret mapping, ensure that your secrets and Request Servers are created and set up in PAM.

### Adding or Updating a Secret Mapping

To add or update a Secret Mapping, complete the following procedures as the PAM Administrator:

1. Select **Secrets, Manage Secret Authorizations**
2. The Secret Authorizations page lists the existing mappings. If an entry shows as a plain name then it is a single secret. If the entry shows () around the name, then it is a secret group. See [Using Groups for Authorization](#) for information about secret groups.
  - a. To add a new mapping, click **Add**. The Add Secret Authorization Mapping modal appears
  - b. To update an existing mapping, select the map from the list to be updated and click **Edit**. The Update Secret Authorization Mapping modal window appears.
3. Select whether to add a secret group (Group) or a single secret (Alias). Then, enter the target group or alias name, or search for a target group or alias using the magnifying glass.
4. Select a Requestor Server Group (Group) or Requestor Server (Client). Then, enter the requestor group or client name, or search for an A2A requestor group or client using the magnifying glass.
5. The mapping can perform a series of additional security checks to further lock down what processes on the Request Server can access the secret. These are optional. See [Configure A2A Authorization Mappings](#) for more information.
6. Select **OK** to save the mapping.

### Deleting a Secret Mapping

Deleting a secret mapping removes it permanently from PAM. You cannot restore a deleted secret mapping. However, the secrets and the Request Server assigned to the secret mapping are not deleted.

To delete a secret authorization mapping:

1. Select **Secrets, Manage Secret Authorizations**.
2. Select the secret mapping that you want to delete and click **Delete**.
3. When prompted to confirm the action, click **Yes**.

## Using Secret Groups for Authorization

Authorizing a Request Server to access a single secret is a fine-grained way to manage authorizations using secret mappings. Although PAM supports this use scenario, it can become cumbersome and difficult to manage. For ease of management, a PAM administrator may choose to group a set of secrets (a secret group), a group of Request Servers (a request group), or both. Using groups lets the administrator apply authorization policies to multiple secrets and Request Servers more easily.

A group is a collection of secrets or Request Servers that meet specific filter criteria; for example, all secrets that have the identifier SSL in the Descriptor2 field. A single secret or Request Server might belong to multiple groups.

PAM supports two types of groups:

- Static groups allow PAM Administrators to choose explicitly what is in the group. Group contents do not change over time.
- Dynamic groups allow PAM Administrators to choose a set of rules which the request references to determine if something is in or out of the group.

Dynamic secret groups apply a logical *or* relationship for filters that use the same attribute. For example, if a group contains a vault filter with the Description1 “Test” and a vault filter for the Description1 “Production”, the resulting group contains all secrets with either *Test* or *Production* in their description.

Filters that use different attributes are applied using a logical *and* relationship. For example, if a group contains a vault filter for the Description1 “Production”, and a Secret filter in Description2 with “SSL”. The resulting group contains only secrets with *Production* in Description1 and *SSL* in the Descriptor2 field.

On the pages where groups are defined, there is a **Show** button that provides a preview of the resulting data. This preview gives PAM Administrators the ability to check the results before saving.

### **Guidelines for Mapping Secret Groups**

When you create a Dynamic Secret Group, the group contains all Secrets that satisfy the filter criteria. When you map a Secret Group that includes filters, be aware of how you set the Check Execution Path and Check File Path check boxes:

- If you select one or both check boxes, the authorization mapping is restricted to only those secrets that are in the database. The authorization mapping excludes any secrets that are not in the database.
- If you clear the check boxes, all secrets in the group are included in the authorization mapping.

### **Adding or Updating a Secret Group**

1. Select **Secrets, Manage Secret Groups**.
2. On the Secret Groups page:
  - To add a new secrets group, click **Add**. The Secret Group modal appears.
  - To update an existing secret group, select the group to update and click **Update**. The Update Secret Group modal appears.
3. Enter a Name and optionally a Description to identify this secret group and click **OK**. The group name must be unique.
4. Select whether the group is dynamic or static from the Type drop-down.
5. Add filters to the group. Repeat this procedure for each filter you want to add.
  - a. Select the **Not Specified** link for the filter that you want to apply. The Define Filters dialog appears.
  - b. Select the plus icon (+) to add an expression.
  - c. Select the filter type (for example, *contains*) from the drop-down list in the Operator field.
  - d. Enter the filter expression (for example, *SSL*) in the Value field.
6. Select **OK** to save your changes.

### **View All Secrets Belonging to an Existing Secret Group**

Use the following procedure to view all secrets belonging to an existing secret group:

1. Select **Secrets, Manage Secret Groups**.
2. On the Secret Groups page, select the target group that you want to view and select **Update**.
3. Select **Show**. The list of groups matching the criteria within the group displays.
4. Switch between the Vaults, Secret Types, and Secrets tabs to view detailed information about the secrets that are assigned to this group.

5. Select **OK**.

### **Copying a Secret Group**

To copy a secret group into your clipboard:

1. Select **Secrets, Manage Secret Groups**.
2. Select the secret group that you want to copy and click **Update**. The Copy Secret Type modal appears.
3. Modify the secret group as required and click **OK** to save this secret group as a new secret group.

### **Deleting a Secret Group**

Deleting a secret group removes it permanently from PAM. You cannot restore a deleted secret group. However, the secrets that are assigned to the group are not deleted.

To delete a secret group:

1. Select **Secrets, Manage Secret Groups**.
2. Select the secret group that you want to delete and click **Delete**.
3. When prompted to confirm the action, click **Yes**.

## Implementing PAM SC

---

The topics in this section provide end-to-end instructions for configuring the unified PAM Integrated Server Control functionality, with a strong emphasis on migration from existing PIM or PAM SC implementations:

- [PAM SC Unification Overview](#)
- [PAM SC Guided Workflows](#)
- [Install And Configure PAM SC Utility Appliances](#)
- [Migrate From PIM or PAM SC to PAM](#)
- [Upgrade and Migrate PIM and PAM SC Endpoints](#)
- [Associating PAM SC Devices with PAM Devices](#)
- [Install PAM SC Endpoints](#)
- [Server Control Configuration Settings](#)
- [High Availability](#)
- [Configure PAM SC to Protect Your Endpoints](#)
- [Administrate PAM SC](#)
- [Troubleshoot PAM SC](#)
- [PAM SC reference](#)

### PAM SC Unification Overview

This content introduces the features and benefits of unifying the PIM and PAM Server Control (formerly the standalone Privileged Access Manager Server Control product) into Privileged Access Manager.

#### **Privileged Access Manager (PAM)**

PAM enables centralized management of local and remote high-risk users over traditional physical hardware, virtual, and cloud environments.

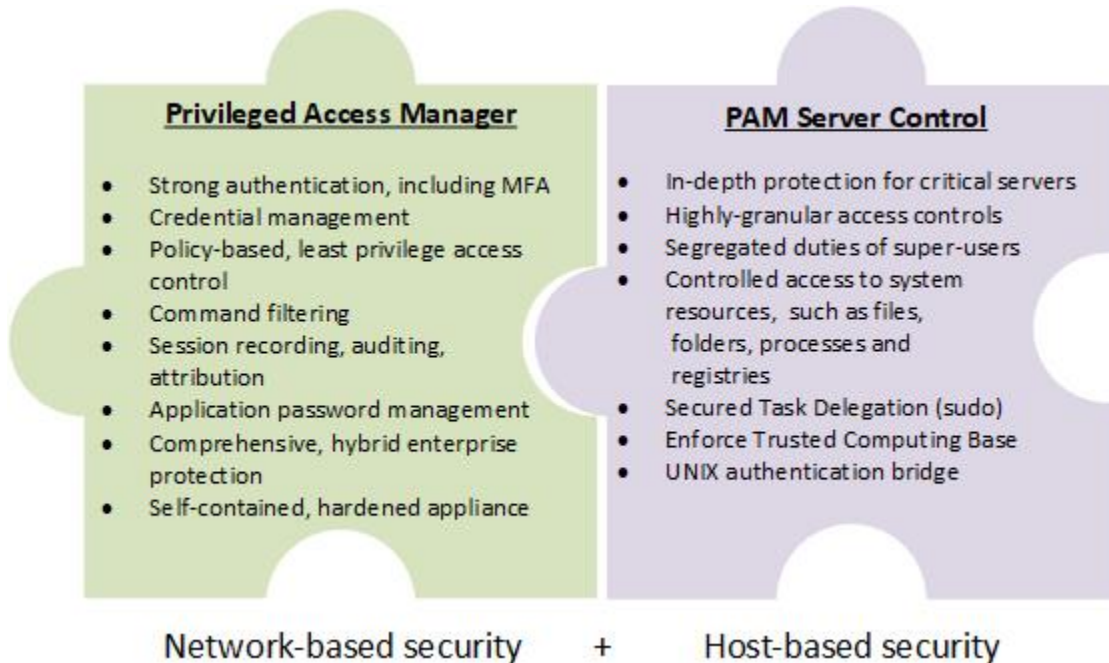
#### **Privileged Identity Manager (PIM) and Privileged Access Manager Server Control (PAM SC)**

The PIM and PAM SC products provide comprehensive solutions for protecting the most critical business assets — your mission-critical servers. These products provide powerful, fine-grained protection over operating system-level access and privileged user actions. PIM and PAM SC are system-level, host-based solutions that:

- Control, monitor, and audit privileged user activity to improve security.
- Reduce administrative costs.
- Simplify audit and compliance processes across physical and virtual environments.

#### **Unification Overview**

The PAM server now includes a *Server Control Module* that unifies the capabilities of PIM and PAM SC, adding powerful host-based security to its existing comprehensive network-based security. This combination of capabilities is shown in the following diagram:



### **Unification Highlights**

The following sections describe the unification-related functionality in more detail:

#### ***Migration Utility to Migrate PIM or PAM SC DMS Data to PAM***

This release includes a Migration Utility wizard that migrates DMS data (Devices, Device Groups, Policies, and Deployments) from existing PIM and PAM SC environments to PAM. Migration involves the following tasks:

- Extraction
- Validation
- Backing up PAM
- Migrating the PIM or PAM SC data
- Finalizing the process

#### ***New PAM Distribution Server Utility Appliance***

This release provides a new hardened *Distribution Server Utility Appliance* that runs the software necessary to deploy and support PIM and PAM SC Distribution Server functionality.

#### ***PIM and PAM SC Policy Deployment Integrated Into the PAM UI***

Policy deployment functionality allows you to deploy fine-grained access policies to the Endpoint Agents from the PAM UI. The following lists show the operations that you can perform:

#### **Policy CRUD Functionality**

- Add
- Copy
- Update
- Delete

#### **Policy Management Functionality**



- Assign
- Unassign
- Upgrade
- Downgrade

### ***UNIX Authentication Broker (UNAB)***

The UNIX Authentication Broker (UNAB) consists of several components that manage and control access to the UNIX host by Active Directory users. You can manage the following UNAB functions through PAM:

- **UNAB Login Authorization - Host or Host Group**

From the PAM UI, you can control users and groups access to the UNIX hosts and can configure your UNAB host. You can also control user and group access to the UNIX host by granting access to only those users and groups that are permitted to log into that host.

- **Configure a UNAB Host or Host Group**

From the PAM UI, you can change the configuration files of a UNAB host or hosts (belonging to a host group) by deploying UNAB configuration policies.

### ***Role-Based UI Allows Segregation of Duties***

In the PAM UI, you assign privileges to users and administrators by assigning admin and privileged access roles. A role contains tasks that correspond to application functions in PAM.

Roles simplify privilege management. Instead of associating a user with each task that they perform, you can assign a role to the user. The user can perform all the tasks in their assigned role. Every user who has the role can now perform the new task.

When a user logs in to PAM, the user sees only the tabs and tasks that are assigned to their role. You can assign separate roles to different users to prevent one user being able to complete every task. This feature allows your organization comply with separation of duties requirements.

List of available roles:

- Server Control Administrator
- Server Control Policy Editor
- Server Control Deploy Manager
- UNAB Manager

### ***Agent Status Dashboard***

The **Agent Status Dashboard** allows users to check the status (Active, Inactive, and warning) of PIM and PAM SC devices (Agent, UNAB, and PUPM). Once the devices are migrated to PAM, the exact count of existing PIM and PAM SC devices that are displayed in the **PAM Device Agent** summary under **Uninitialized** is accurate. Once the cutover is done, the device count is always shown under the corresponding agent type.

### ***API-Based Policy Management***

Use PAM APIs to automate management of CA PAM/PIM policies (Policy CRUD and Policy Manage) without the need to use the PAM UI.

### ***(SIEM) Track User Behavior Activities on Server Control Devices on PAM***

Use this functionality to track all the activities and events that are performed on all Server Control Devices. These events can be viewed through a third-party tool such as Splunk and ArcSight.

### ***Login Integration With the New Virtual Appliance Distribution Server***

Login integration assists you to audit the actual user of your server, not just the shared local privileged user name. Privileged Access Manager Server Control Login Integration allows PAM to integrate the login process and

information with Server Control. When activated, it allows the use of the actual user name for auditing in Privileged Access Manager Server Control.

### ***Simplifies Agent Installation and Upgrades***

Unified Server Control allows you to simplify PIM and PAM SC Endpoint installations, upgrades, and patches with *no* downtime and provides a rollback mechanism if there is failure. This simplification reduces the time to deploy from several months to days.

Simplified agent installation is supported on all Linux implementations, as shown in the following list:

- YUM Package Manager: OEL, SLES, RHEL
- APT-GET Package Manager: DEBIAN, UBUNTU

### **Introducing the Utility Appliance (Which Replaces Distribution Servers)**

In the PAM environment, PAM SC Distribution Servers are replaced by *Utility Appliances*. These Utility Appliances are VMware, AWS, or Azure virtual machines that you can freely download and deploy. Utility Appliances host preloaded Distribution Server software that is backwards-compatible with the PIM and PAM SC endpoint agents that are currently installed on endpoints.

#### **NOTE**

#### **Why was the Distribution Server replaced by the Utility Appliance?**

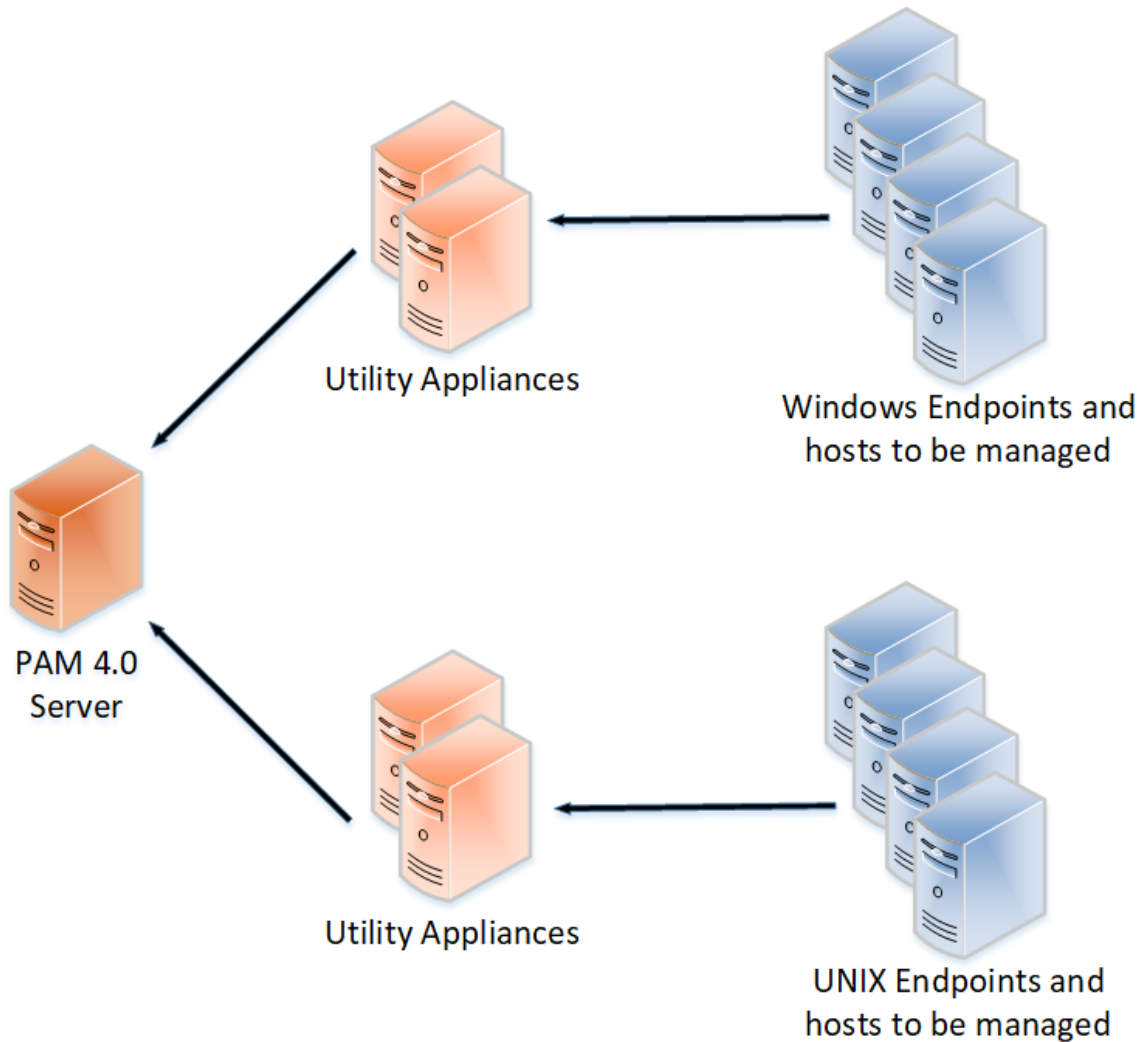
First, each PAM SC Distribution Server held a full copy of all information from across *all* endpoints, causing a noisy and data-intensive communication paradigm.

By contrast, the Utility Appliance only caches information about the Server Control devices to which it is connected. When data changes (for example, a new device is assigned), the cache for that device is invalidated and the next request by the device fetches updated information.

This model reduces the overall traffic between the components and streamlines data delivery. These features allow you to configure a more frequent polling time and therefore deliver policies more quickly to the devices.

Second, the adjusted communication method provides the opportunity to support larger sets of Server Control devices. Third, with the new Utility Appliances, you can deploy, configure, and run Distribution Software within minutes, significantly reducing the time and effort to expand capacity.

Like PIM and PAM SC Distribution Servers, Utility Appliances sit between PAM and the *devices* (formerly known as endpoints) that are under Server Control management, maintaining scale and Endpoint load distribution. The PAM implementation also provides optimized communication between PAM and the Utility Appliance, and between the Utility Appliance and the endpoints. The following diagram shows the basic architecture.



Further information in

this section

**TIP**

See the following topics in this section for more detailed information

- [Server Control Components in PAM](#)
- [PAM Unified Server Control Functional Overview and Business value](#)
- [Technical Specifications](#)

:

## Server Control Components in PAM

This content describes the Server Control-related components in the unified PAM solution.

### PAM Server

The Server Control module makes the PAM Server the central management server for all Server Control functions. The Server Control module replaces the Enterprise Management Server in the standalone PIM and PAM SC products. The Server Control module includes components and tools that allow you to:

- Deploy policies to endpoints
- Define resources
- Define accessors
- Define access levels

### **Utility Appliances**

In the PAM environment, PIM and PAM SC Distribution Servers are replaced by *Utility Appliances*. The Utility Appliances are VMware, AWS, or Azure virtual machines that you can freely download and deploy. Utility Appliances host preloaded Distribution Server software that is backwards-compatible with PAM SC Endpoint Agents that are currently installed on endpoints. Like the PAM appliances, the Utility Appliances are hardened. PAM protects and controls access to these appliances.

#### **NOTE**

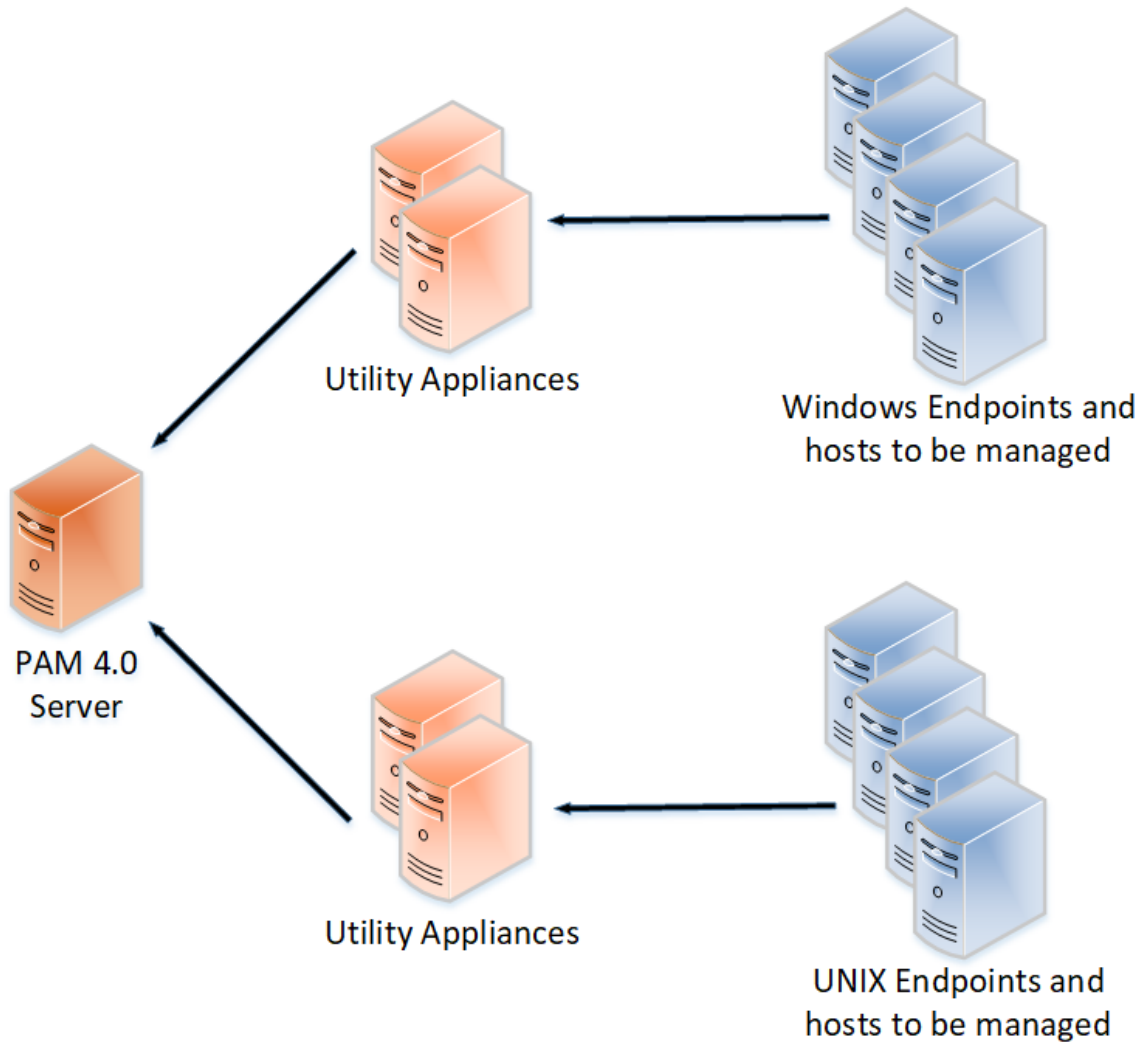
##### **Why was the Distribution Server replaced by the Utility Appliance?**

Each PAM SC Distribution Server held a full copy of all information from across *all* endpoints, causing a noisy and data-intensive communication paradigm.

By contrast, the Utility Appliance only caches information about the Server Control devices to which it is connected. When data changes (for example, a new device is assigned), the cache for that device is invalidated and the next request by the device fetches the updated information.

This model reduces the overall traffic between the components and streamlines data delivery. These features allow you to configure a more frequent polling time and therefore deliver policies more quickly to the devices.

Like PIM and PAM SC Distribution Servers, Utility Appliances sit between PAM and the endpoints that are under Server Control management, maintaining scale and Endpoint load distribution. The PAM implementation also provides optimized communication between PAM and the Utility Appliance, and between the Utility Appliance and the endpoints. The following diagram shows the basic architecture:

**NOTE**

For failover purposes, deploy multiple Utility Appliances in your enterprise. You can place a load balancer between the Server Control Devices and the Utility Appliances under a Source IP algorithm. Load balancers are not provided as part of the PAM infrastructure.

**Server Control Agent**

The Server Control Agent is a powerful tool for managing security for your native platforms, allowing you to set up the following capabilities:

- Implement a customizable security policy to meet the security requirements of the enterprise
- Provide security for users, groups, and resources beyond what is available in native operating systems
- Centrally manage security across the organization and integrate your Windows and UNIX security policies in a heterogeneous environment

## **UNIX Authentication Broker (UNAB)**

UNIX Authentication Broker (*UNAB*) allows you to log in to UNIX computers using an Active Directory data store. This functionality means that you can use a single repository for all your users. Your users can log in to all platforms with the same username and password.

Integrating UNIX accounts with Active Directory enforces strict authentication and password policies and transfers the rudimentary UNIX user and group properties to Active Directory. This integration allows you to manage UNIX users and groups in the same location that you manage Windows users and groups.

In the unified PAM solution, you manage your UNAB hosts from the PAM UI, from where you can:

- Control Active Directory users' access to every UNAB host in the enterprise.
- Manage hosts' login authorizations.
- Resolve hosts' migration conflicts.
- Generate reports.
- Create login authorization and configuration policies for UNAB devices and device groups. Login authorization policies permit or revoke authorization to Active Directory users and user groups on UNAB devices and device groups.

UNAB consists of two components that manage and control access to UNIX hosts by Active Directory users:

- **UNAB Authentication Agent:** Services and maintains a secure connection with Active Directory to provide the following functionality:
  - User authentication and login authorization
  - Host registration with Active Directory
  - User and group migrations
  - Administering local access files
- **uxconsole:** A UNAB management console to register the UNIX host with Active Directory, migrate users and groups and to register and activate UNAB.

## **Endpoint Software**

PAM SC provides software for two types of Endpoint agents:

- **Endpoint Agents**  
Install PAM SC Endpoint Agent software on Windows and UNIX servers that you want to secure with PAM SC.
- **UNAB Authentication Agent**  
Install the UNAB Authentication Agent on UNIX servers with an Active Directory data store that you want to act as a single repository for all of your users.

## PAM Unified Server Control Functional Overview and Business value

This topic provides a detailed functional overview and presents the business value of PAM with unified Server Control functionality.

Problem Statement	Solution
<p>Many data breaches happen because of compromises in privileged user accounts, such as UNIX/Linux superuser account (root) and Windows administrator accounts. Privileged user accounts provide full, unauthorized access to all applications, data, and audit logs for exploitation. As a result, malicious insiders and external hackers specifically target these accounts.</p> <p>Unfortunately, these superuser accounts cannot be disabled because systems administrators need the privileges to perform necessary and legitimate maintenance of critical servers. Extra protections that audit all access, identify, and prevent unauthorized activities, while still allowing legitimate actions, are key to defending mission-critical servers. Just one improperly authorized privileged account usage can cause widespread, irreparable damage to the infrastructure, intellectual property, and brand equity for exploitation of your organization.</p> <p>You need a proven privileged access management solution that provides powerful controls over privileged users on your most critical systems.</p>	<p><b>Use PAM</b></p> <p>Integration of CA Privileged Access Manager Server Control with PAM is a comprehensive and mature solution that is designed to protect your most sensitive systems whether they are physical, virtual, or cloud.</p> <p>CA Privileged Access Manager is a scalable solution capable of deploying fine-grained access controls, auditing, and UNIX authentication bridging across servers from a single PAM control plane. PAM is also uniquely capable of deploying policies that enforce access kernel-level controls on any account, such as UNIX root and Windows administrator.</p>
<p>The Security Administrators in two different divisions of a company have come to you for assistance in developing consistent security policies across the divisions.</p>	<p><b>Deploy Policies</b></p> <p>The three Security Administrators have decided to deploy a PAM 4.0 environment to establish centralized propagation of vaulting and security rules. With PAM 4.0, you can create and deploy a policy to the agents distributed across your entire company or enterprise.</p>
<p>You are a Security Administrator for the Manufacturing Division of Example.com. Now that management has decided to implement an enterprise-wide security solution, your task is to install the application.</p>	<p><b>Install PAM</b></p> <p>Set up the system for installation. Install PAM 4.0 Appliance. Verify the installation.</p>
<p>You are the Security Administrator for PIM and PAM SC, and management has decided to consolidate security tools into a single platform: PAM. As the owner of this application and project, and to cause minimal business disruptions, you want:</p> <ul style="list-style-type: none"> <li>• An automated way to transfer the data into PAM</li> <li>• A controlled way to roll out this change.</li> </ul> <p>You should still be able to access all existing fine grained policies, devices, devices groups, and deployments from the PAM UI.</p>	<p><b>Use the Migration Utility</b></p> <p>The Migration Utility allows you to migrate the DMS data (Devices, Device Groups, Policies, and Deployments) from the existing PIM environment to PAM. Migration does the following tasks:</p> <ul style="list-style-type: none"> <li>• Extraction</li> <li>• Validation</li> <li>• Backup PAM</li> <li>• Migrate Data</li> <li>• Finalize Process</li> </ul>
<p>You are a Security Administrator. Now that you want to deploy Server Control or fine-grained policies across multiple agents, you need Distribution Server software which is easy to install and scalable.</p>	<p><b>Utility Appliance</b></p> <p>The new Utility Appliance is a hardened all-in-one virtual appliance that provides all Distribution Server functionality.</p>

<p>The Example.com security policy requires least privilege and separation of duties, requiring the following restrictions:</p> <ul style="list-style-type: none"> <li>Each user has only the access that is required to perform their job.</li> <li>No single user has access to all security functional areas.</li> </ul> <p>Your primary concern is policy management functionality. When you log into PAM as a user with Server Control privileges, you should see the aspects of the UI and functionality that is related to your role. Similarly, users should see only the tabs and tasks that are assigned to their role.</p>	<p><b>Role-based UI</b></p> <p>You can assign users in PAM entitlements in privileges, which are known as roles, that enable and can disable different options within the PAM UI.</p> <p>Roles simplify privilege management. Instead of associating a user with each task that they perform, you can assign a role to the user. The user can perform all the tasks in their assigned role. Every user who has the role can now perform the new task.</p> <p>When a user logs in to PAM, the user sees only the tabs and tasks that are assigned to their role. You can assign separate roles to different users to prevent one user being able to complete every task. This feature allows your organization to comply with separation-of-duties requirements.</p> <p>List of roles:</p> <ul style="list-style-type: none"> <li>Server Control Administrator</li> <li>Server Control Policy Editor</li> <li>Server Control Policy Manager</li> <li>UNAB Manager</li> </ul>
<p>You are a Security Administrator of Example.com. As a Security Administrator, you would like to know and understand the health and status of your different agents.</p>	<p><b>Agent Status Dashboard</b></p> <p>Agent Status Dashboard only applies to Server Control-based devices. The Agent Status Dashboard allows users to check the Status (Active, Inactive, Warning) across each of the different Agent types (Server Control, UNAB, PUPM).</p> <p><b>Note:</b> During a migration from PIM/PAM SC, Agents might be listed as "Uninitialized". This status is expected until the final cutover occurs, and then PAM starts managing this data.</p>
<p>As a Security Administrator, you want to automate the policy deployment without having to log in to the PAM UI.</p>	<p><b>Policy Management through API</b></p> <p>The PAM APIs for Server Control policy management functionality (Policy CRUD and Policy Manage) allow Security Administrators to automate without using the PAM UI.</p>
<p>You are a Security Administrator, and you want to track and audit the actual user of your server, not the shared local privileged user name.</p>	<p><b>Login Integration</b></p> <p>Login integration helps you to audit the actual user of your server, not the shared local privileged user name. Privileged Access Manager Server Control Login Integration allows Privileged Access Manager to integrate the login process and information with Server Control. When activated, it allows the use of the actual user name for auditing in Privileged Access Manager Server Control.</p>
<p>As a Security Administrator for the Manufacturing Division of Example.com, you have a deadline to upgrade from existing PIM endpoints to PAM SC/PIM, but you have a concern that it might take several months.</p>	<p><b>Simplified Agent Installation and Upgrades</b></p> <p>This functionality allows you to simplify endpoint installations, upgrades, and patches with NO downtime. This functionality includes rollback mechanism in case failures occur. This simplification reduces the time to deploy from several months to days.</p> <p>This functionality supports all Linux variants:</p> <p>YUM Package Manager: OEL, SLES, RHEL</p> <p>APT-GET Package Manager: DEBIAN, UBUNTU</p>
<p>The Example.com corporate security policy mandates a daily audit to monitor critical hosts for user activity security breaches and attempted security breaches. As a security Administrator, you want to see all the Audit events in a centralized UI.</p>	<p><b>(SIEM) Track User Behavior Activities on Server Control Devices</b></p> <p>As System Administrator, you decide to log in to the PAM server to configure the SIEM tool information. Next, you log in to the Server Control device to run the Report Agent. The agent then sends the snapshot to Splunk, where you can view the User Activity reports.</p>



Example.com, wants to consolidate user stores across windows and UNIX hosts. Their goal is to enable Active Directory-based UNIX logins.

#### UNAB

PAM offers the UNIX Authentication Broker to authenticate UNIX users against Active Directory. UNAB must be installed and configured for UNIX users to be able to log in with their AD credential. With AC UNAB Authorization, the administrators can authorize users and groups to host or host groups. With AC UNAB configuration, the administrators can manage UNAB configuration settings. Host or host groups can be managed using this feature.

## Server Control Concepts

In the PAM-integrated solution, Server Control refers to fine-grain control enforcement.

To establish fine-grain control, assign a Server Control policy to a device or group of devices.

- **Server Control Policy:** A Server Control Policy is a set of rules that are enforced within the kernel of the device. Server Control Policies are authored and managed in PAM using the UI and API. Versions of Policies are managed within PAM; however, once a policy is finalized, it cannot be changed.
- **Device and Device Group:** In PAM, devices can be grouped into Devices and Device Groups, saving management overhead for authorization. Similarly, for Server Control functionality, individual devices or groups of devices can be assigned Server Control policies. As in previous versions of PAM, device group membership can be managed directly in PAM or imported from an external source.
- **Assignment:** An Assignment is an instruction stating that a version of a policy is assigned to a device or device group. A device or device group is often assigned one or more policies.

## PIM/PAM SC Component Changes in PAM 4.0

The following table compares the key components and functions in PIM and PAM SC to their functional equivalents in PAM 4.0.

PIM/PAM SC	PAM 4.0	Notes
Enterprise Manager (ENTM) centralized management platform	PAM Server	PAM facilitates policy and deployment changes.
Distribution Server	Utility Appliance	The Utility Appliance is a black-box, PAM-managed device that runs the Distribution Server software. The Utility Appliance handles communication between PAM and the endpoints. For scalability and to manage endpoints that are located behind firewalls, install more Distribution Servers in your enterprise.
Policy Model Database (PMDb)	Utility Appliance	In PIM/PAM SC, the PMDB plays a critical role in distributing data to endpoints connected to it. In PAM 4.0, the functionality in the Utility Appliance significantly changes the role of the PMDB. <b>Direct access to PMDB on the Utility Appliance is not allowed in PAM 4.0.</b>
Endpoint Agents	Endpoint Agents	No software changes needed. In PAM 4.0, endpoint agents can be deployed using package managers (for example, yum or apt).
	Migration Tool	A multi-staged utility to extract data out of PIM/PAM SC and add that data into PAM.

## Server Control Roles in PAM

Server Control user roles support separation-of-duties requirements. As with any capability or role within PAM, you can choose to combine them for a desired operational state.

The following list describes the Server Control roles and the privileges that they provide:

- **Server Control Policy Editor:**
    - Full access to Server Control policy features, including create, update, version, and finalization process.
  - **Server Control Deploy Manager:**
    - Full access to policy deployment features, including assign, unassign, upgrade, and downgrade.
    - Read-only access to devices/device groups and server control policies.
  - **Server Control Administrator:**
    - Access to the Dashboard Overview, Device Agent Status, Session Logs, Device / Device Groups, Device Tags, Server Control Policy, Policy Deployment, and Deployment audit.
- NOTE**  
The Dashboard System Tab is not available for users with the Server Control Administrators role.
- Full access to UNAB policy management, UNAB Configuration, and token management capabilities on devices and device groups. Access to users and user groups.
  - **UNAB Manager:**
    - Full Access to UNAB host login policy management and UNAB configuration token management on devices and device groups.

## How Server Control Works

This content describes how the existing PAM and new PAM SC components work together.

### PAM Server

The PAM Server is the central source of information. Server Control information is shared across the PAM cluster and is available from wherever PAM is accessible.

Policies can be drafted, saved, and edited as often as needed on the PAM Server. However, when a policy is *finalized*, it cannot be changed.

Assignments indicate that a policy or policies are consigned to a device or a device group.

### Endpoint

The endpoint software running on a device requests for and receives assignments and corresponding policy details and instructions. The agent incorporates these instructions into its processing engine, where they become the enforcement rules.

### Utility Appliance with Distribution Server Software

To help with the scale and regional distribution, PAM provides a hardened virtual Utility Appliance that hosts improved Distribution Server software. The Distribution Server software helps distribute the load and improve the communication traffic.

The Distribution Server software is backwards-compatible, so no upgrade of any currently installed endpoint agent is required.

## Technical Specifications

### Recommendations for single-site or small environment production workloads:

#### NOTE

These suggested numbers depend on the eventual size of your deployment. See the Sizing Guide for additional information.

Count	Type	RAM	Disk	Cores
3	PAM	16 GB	120 GB	8
N	PAM Utility Appliance	16 GB	40 GB	8

### Recommendations for multi-site environment production workloads:

Count	Type	RAM	Disk	Cores
6	PAM (2 sites)	16 GB	120 GB	8
N	PAM Utility Appliance	16 GB	40 GB	8

## PAM SC Guided Workflows

The topics in this section contain high-level guided workflows.

Use the table of contents to access the individual workflows.

### Guided Workflow: Migrate a PIM or PAM SC Environment to PAM

This guided workflow provides a high-level overview of how PIM and PAM SC administrators can adopt PAM. This content also summarizes the technical and business value from your point of view, where applicable.

	Step	Description
1	Complete prerequisites before migrating from PIM or PAM SC to PAM	Required preparation for migrating from PIM or PAM SC to PAM. See <a href="#">Prepare to Migrate to PAM</a> for details.
2	Upgrade existing PAM servers to 4.x or deploy new PAM 4.x servers.	All the PAM servers in your cluster must be running version 4.x. Upgrade existing PAM servers to 4.x or deploy new PAM 4.x servers. See <a href="#">Upgrading</a> or <a href="#">Deploying</a> for details.
4	License PAM to support Server Control.	Server Control is a separately licensed PAM component. See <a href="#">License PAM to Support Server Control</a> for details.
3	Download and Deploy Utility Appliances.	Utility Appliances are VMware virtual machines that host the Distribution Server software that stands alone in PIM and PAM SC. Download and deploy at least one Utility Appliance before proceeding with the adoption process. See <a href="#">Download and Deploy a New Utility Appliance</a> for details.
5	Add and activate Utility Appliances in PAM	To configure PAM to communicate with and activate Utility Appliances, do the following steps: <ol style="list-style-type: none"> <li><a href="#">Create Utility Appliance devices.</a></li> <li><a href="#">Add the Utility Appliance devices to Utility Groups.</a></li> </ol> PAM creates a cluster from the Utility Appliances in a Utility Group, starts the Utility Appliances, which then start communicating with PAM.
6	Migrate data from CA PIM to PAM.	Install and run the Migration Utility on an Enterprise Management Server to migrate the PIM or PAM SC data to PAM. See <a href="#">Migrate Data from PIM or PAM SC to PAM on Windows</a> or <a href="#">Migrate Data from PIM or PAM SC to PAM on Linux</a> for details.

7	Verify that all your PIM/ PAM SC endpoint agents are present in the PAM environment.	Once your devices are migrated to PAM, verify that the exact count of existing PIM or PAM SC endpoint devices is shown in the <b>Agent Status Summary</b> screen as Uninitialized. Once the cutover is complete, each agent is listed under its respective agent type. See <a href="#">View Server Control Endpoint Agent Status on the Device Agent Status Screen</a> for more details.
8	Configure endpoints to connect to Utility Appliances, manage endpoints with PAM.	Configuring endpoints to connect to Utility Appliances and managing endpoints with PAM enables the cutover of server control devices from PIM or PAM SC to PAM. See <a href="#">Post Migration Steps</a> for details.
9	Troubleshoot extraction and validation errors.	If you have extraction or validation errors, and the problem is not immediately obvious, see <a href="#">Troubleshooting and Maintenance</a> and <a href="#">Troubleshoot Orphaned Data, Records, and Validation Errors</a> for information about how to solve these issues: <ul style="list-style-type: none"> <li>• Identify extraction errors</li> <li>• Fix orphan data</li> <li>• Identify validation errors</li> <li>• Review the reasons for failures</li> <li>• Fix records in the JSON File</li> </ul>
10	Assign user roles to specify segregation of duties.	To perform Server Control operations in PAM, a user must be assigned one or more of the following roles, which were designed to support separation of duties, if desired. <b>Server Control Policy Editor</b> Full access to Server Control policy creation, updates, version, and finalization process Read-only Access to device and device groups, policy deployment, and deployment audit features <b>Server Control Deploy Manager</b> Full access to policy deployment features, including assign, unassign, upgrade, and downgrade. Read only Access to device/device groups and server control policies <b>Server Control Administrator</b> Full access to Device/Device groups, Device tags, Server Control Policy, policy deployment and deployment audit Full access to UNAB policy management, UNAB configuration, and token management capabilities on devices and device groups. Access to users and user groups <b>UNAB Manager</b> Full Access to UNAB Host Login policy management and UNAB configuration token management on devices and device groups For more information, see <a href="#">Identify User Roles and Privileges</a> .
11	Use the Server Control Policy Editor	Create, copy, update, and delete Server Control Policies that may or may not be sent to and enforced on a Server Control Device or Server Control Device Group. For more information, see <a href="#">Manage and Troubleshoot Server Control Policies</a> .
12	Assign, unassign, upgrade, and downgrade Server Control Policies.	To implement the policy rules, assign the latest, finalized policy version to specific Devices or Device Groups. Assigned policies are automatically deployed. Once deployed, you can then monitor the policy's deployment status. You can also unassign a specified policy from one or more hosts or host groups. New policy versions are not automatically sent to assigned hosts or to hosts with a deployed policy. You must manually upgrade hosts where the policy is deployed to the latest policy version. If you either inadvertently assign the wrong policy version to one or more hosts, or if you want to go back to an older version of a policy on specific hosts, you can downgrade a policy. For more information, see <a href="#">Advanced Server Control Policy Management</a> .
13	Policy Management using the PAM External API	Use the PAM External API to manage your Server Control policies programmatically, which allows you to automate the process without using the PAM UI. For more information, see <a href="#">PAM External REST API</a> .

14	Configure PAM to track user activities on Server Control devices or viewing in a SIEM Tool.	To track all activity and events that are performed on your Server Control devices for IT governance purposes, configure PAM to report them to a <i>Security information and event management (SIEM)</i> tool such as Splunk or ArcSight. For more information, see <a href="#">Track User Behavior Activities on Server Control Endpoints Using an SIEM Tool</a> .
15	Login integration with new Distribution Server	Login integration helps customers to audit the actual user of your server, not the shared local privileged user name. PAM Server Control Login Integration allows PAM to integrate the login process and information with Server Control. When activated, it allows the use of the actual user name for auditing in PAM Server Control. For more information, see <a href="#">Configure Login Integration for a Server Control Endpoint</a> .

## Guided Workflow: Migrate a PIM or PAM SC Environment with UNAB to PAM

This guided workflow provides a high-level overview of how PIM and PAM SC administrators whose PIM or PAM SC deployments include UNAB can adopt PAM 4.0. This content also summarizes the technical and business value from your point of view, where applicable.

Your UNAB host should be the same host on which you install PAM SC.

	Step	Description
1	Install and configure the PAM SC UNIX Attributes plug-in	Install and configure the PAM SC UNIX Attributes plug-in on your UNAB host. The plug-in lets you manage UNIX attributes for UNAB users on Active Directory: <ul style="list-style-type: none"> <li><a href="#">Install the CA Privileged Access Manager Server Control UNIX Attributes Plug-in</a></li> <li><a href="#">Configure UNIX Attributes for an Active Directory User</a></li> </ul>
2	Configure your Active Directory (AD)	Configure your AD to work with your UNAB host: <ul style="list-style-type: none"> <li>Configure your AD with forward and reverse lookups for your UNAB endpoint.</li> <li>Your AD must have existing users. At least one user must have account membership in a group that permits that user to perform administrative tasks.</li> </ul> See the documentation that came with your Active Directory for details.
3	Install UNAB Agents (Standalone)	Install and configure the UNAB Agents: Install a UNAB Agent on the PAM server to get granular access to AD users. <ul style="list-style-type: none"> <li><a href="#">Install and Configure UNAB Agent</a></li> <li><a href="#">UNAB Agent Post Installation Configuration</a></li> </ul>
4	Upgrade or install PAM SC Endpoint Agents	If not already installed, install the PAM SC Endpoint Agents: <ul style="list-style-type: none"> <li><a href="#">Install a CA PIM or PAM SC Endpoint Windows</a></li> <li><a href="#">Install a Server Control Agent on a UNIX Endpoint</a></li> <li><a href="#">Installing and Uninstalling Endpoint Agents Using YUM</a></li> </ul> Otherwise, upgrade your PAM SC Endpoint Agents. See <a href="#">Upgrade and Migrate PIM and PAM SC Endpoints</a>
5	Verify that users can access the UNAB host	Verify that users can access the UNAB host. With a user in a group that permits that user to perform administrative tasks, run the following command: <pre>uxconsole -manage -show -user &lt;username&gt;</pre>
6	Complete prerequisites for migrating from PIM or PAM SC to PAM	Required preparation for migrating from PIM or PAM SC to PAM. See <a href="#">Prepare to Migrate to PAM</a> for details.
7	Upgrade existing PAM servers to 4.0 or deploy new PAM 4.0 servers.	All the PAM servers in your cluster must be running version 4.0. Upgrade existing PAM servers to 4.0 or deploy new PAM 4.0 servers. See <a href="#">Upgrading</a> or <a href="#">Deploying</a> for details.
8	License PAM to support Server Control.	Server Control is a separately licensed PAM component. See <a href="#">License PAM to Support Server Control</a> for details.

9	Download and Deploy Utility Appliances.	Utility Appliances are VMware virtual machines that host the Distribution Server software that stands alone in PIM and PAM SC. Download and deploy at least one Utility Appliance before proceeding with the adoption process. See <a href="#">Download and Deploy a New Utility Appliance</a> for details.
10	Add and activate Utility Appliances in PAM	To configure PAM to communicate with and activate Utility Appliances, do the following steps: 1. <a href="#">Create Utility Appliance devices</a> . 2. <a href="#">Add the Utility Appliance devices to Utility Groups</a> . PAM creates a cluster from the Utility Appliances in a Utility Group, starts the Utility Appliances, which then start communicating with PAM.
11	Migrate data from CA PIM to PAM.	Install and run the Migration Utility on an Enterprise Management Server to migrate the PIM or PAM SC data to PAM. See <a href="#">Migrate Data from PIM or PAM SC to PAM on Windows</a> or <a href="#">Migrate data from PIM or PAM SC to PAM on UNIX</a> for details.
12	Verify that all your PIM/PAM SC agents are present in the PAM environment.	Once your devices are migrated to PAM, verify that the exact count of existing PIM or PAM SC devices is shown in the <b>Agent Status Summary</b> screen as Uninitialized. Once the cutover is complete, each agent is listed under its respective agent type. See <a href="#">View Server Control Agent Status on the Device Agent Status Screen</a> for more details.
13	Import Active Directory users	Import Active Directory users and groups into PAM, to let PAM discover the selected users and groups from Active Directory. Once discovered, they appear in the PAM UI, letting you manage UNAB login authorization policies. For more information, see <a href="#">Import PIM and PAM SC Active Directory Users into PAM</a> .
14	Assign user roles to specify segregation of duties.	To perform operations in Privileged Access Manager, each user must be assigned one or more user roles, which define sets of privileges that are related to different product functions. This feature allows your organization to comply with separation of duties requirements. Assign one or more of the following roles to each Server Control administrator to specify which operations they can perform: <b>Server Control Policy Editor</b> Full access to Server Control policy creation, updates, version, and finalization process. Read-only access to device and device groups, policy deployment, and deployment audit features <b>Server Control Deploy Manager</b> Full access to policy deployment features including assign, unassign, upgrade, and downgrade. Read-only access to device/device groups and server control policies <b>Server Control Administrator</b> Full access to Device/Device groups, Device tags, Server Control policy, policy deployment, and deployment audit. Full access to UNAB policy management, UNAB configuration, and token management capabilities on devices and device groups. Access to users and user groups <b>UNAB Manager</b> Full Access to UNAB Host Login policy management and UNAB configuration token management on devices and device groups For more information, see <a href="#">Identify User Roles and Privileges</a> .
15	Manage UNAB Login Authorization - Host or Host Group	To control user logins to UNAB hosts or host groups, you create a list of users or groups who are granted access. The list is then formulated into a policy that Symantec PAM assigns and deploys to the selected host or host group. For more information, see <a href="#">Manage UNAB Login Authorization for Devices and Device Groups</a> .
16	Configure a UNAB Host or Host Group	You can define the configuration settings that govern UNAB hosts and host groups. Symantec PAM helps you set the value of the settings in the UNAB configuration file (uxauth.ini) or the configuration file (accommon.ini). After you finish assigning values to the configuration settings, Symantec PAM creates a configuration policy. The policy contains the updated settings values and assigns it to the host or host group. For more information, see <a href="#">Configure a UNAB Host or Host Group</a> .

17	Verify policy deployment from UNAB endpoint	Once policies are deployed from the PAM UI, the same can be verified from the UNAB endpoint. For more information, see <a href="#">Verify Policy Deployment from a UNAB Endpoint</a> .
18	UNAB Policy Management by API	This feature lets you use the APIs for the UNAB management functionality (Login Authorization and configuration) so that they can automate without the need to use the PAM UI. For more information, see <a href="#">Manage Server Control UNAB Policies Using the PAM External API</a> .

## Guided Workflow: Add a New PAM Server Control Implementation to PAM

This guided workflow provides a high-level overview of how to add a PAM Server Control implementation to a new or existing PAM 4.x installation. This content also summarizes the technical and business value from your point of view, where applicable.

	Step	Description
1	If you are not already running PAM 4.x (or later), upgrade an existing installation to 4.x or deploy a fresh one, as appropriate. If you already have an operational PAM 4.x installation, skip this step and proceed to Step 2.	Upgrade an existing PAM installation to 4.x or deploy a new one. For more information, see the <a href="#">Upgrading</a> or <a href="#">Deploying</a> section, as appropriate. All the PAM servers in your cluster must be running the same 4.x version. Once installed, log into the PAM server ( <a href="https://&lt;ip&gt;/cspm/home">https://&lt;ip&gt;/cspm/home</a> ).
2	Download and Deploy PAM SC Utility Appliances.	Utility Appliances are VMware virtual machines that host the Distribution Server software. Download and deploy at least one Utility Appliance. See <a href="#">Download and Deploy a New Utility Appliance</a> for details.
3	License PAM to support Server Control.	Server Control is a separately licensed PAM component. See <a href="#">License PAM to Support Server Control</a> for details.
5	Add and activate Utility Appliances in PAM	To configure PAM to communicate with and activate Utility Appliances, do the following steps: 1. <a href="#">Configure PAM to Communicate with Utility Appliances</a> . 2. <a href="#">Add the Utility Appliance devices to Utility Groups</a> .  PAM creates a cluster from the Utility Appliances in a Utility Group and starts the Utility Appliances, which then start communicating with PAM.
6	Install your PAM SC agents.	Install the PAM SC endpoint agents. See <a href="#">Agent Install or Upgrade</a> .
7	Verify that all your PAM SC agents are present in the PAM environment.	Verify that the exact count of PAM SC devices is shown in the <b>Agent Status Summary</b> screen. Each agent is listed under its respective agent type. See <a href="#">View Server Control Endpoint Agent Status on the Device Agent Status Screen</a> for more details.



10	Assign user roles to specify segregation of duties.	<p>To perform operations in Privileged Access Manager, each user must be assigned one or more user roles, which define sets of privileges that are related to different product functions. This feature allows your organization to comply with separation of duties requirements.</p> <p>Assign one or more of the following roles to each Server Control administrator to specify which operations they can perform:</p> <p><b>Server Control Policy Editor</b> Full access to Server Control policy creation, updates, version, and finalization process. Read only Access to device and device groups, policy deployment, and deployment audit features</p> <p><b>Server Control Deploy Manager</b> Full access to policy deployment features including assign, unassign, upgrade, and downgrade. Read only Access to device/device groups and server control policies</p> <p><b>Server Control Administrator</b> Full access to Device / Device groups, Device tags, Server Control Policy, policy deployment and deployment audit Full access to UNAB policy management, UNAB configuration, and token management capabilities on devices and device groups. Access to users and user groups</p> <p><b>UNAB Manager</b> Full Access to UNAB Host Login policy management and UNAB configuration token management on devices and device groups For more information, see <a href="#">Identify User Roles and Privileges</a>.</p>
11	Create, copy, update, and delete Server Control Policies.	<p>Create a policy to deploy it on any Server Control device or Server Control device group. Copy an existing policy to quickly add a policy with the same properties and then update it as required.</p> <p>Update a policy and create versions only if the previous version of the policy was finalized.</p> <p>For more information, see <a href="#">Manage and Troubleshoot Server Control Policies</a>.</p>
12	Assign, unassign, upgrade, and downgrade Server Control Policies.	<p><i>Assign</i> the latest finalized policy version to specific hosts or to host groups to implement the policy rules. Once assigned, the policy is automatically deployed and you can monitor the policy status from PAM. You can also <i>unassign</i> a specified policy from one or more hosts or host groups.</p> <p>New policy versions are not sent automatically to assigned hosts or to hosts where the policy is deployed. You must manually <i>upgrade</i> hosts where the policy is deployed to the latest policy version.</p> <p>If you inadvertently assign the wrong policy version to one or more hosts, or if you want to go back to an older version of a policy on specific hosts, you can also downgrade a policy.</p> <p>For more information, see <a href="#">Advanced Server Control Policy Management</a>.</p>
13	Policy Management using the PAM External API	<p>Use the PAM External API to manage your Server Control policies programmatically, which allows you to automate the process without using the PAM UI.</p> <p>For more information, see <a href="#">PAM External REST API</a>.</p>
14	Configure PAM to track user activities on Server Control devices or viewing in a SIEM Tool.	<p>To track all activity and events that are performed on your Server Control devices for IT governance purposes, configure PAM to report them to a <i>Security information and event management (SIEM)</i> tool such as Splunk or ArcSight.</p> <p>For more information, see <a href="#">Track User Behavior Activities on Server Control Endpoints Using an SIEM Tool</a>.</p>
15	Configure login integration with a new Utility Appliance.	<p>Login integration helps customers to audit the actual user of your server, not the shared local privileged user name. Server Control Login Integration allows PAM to integrate the login process and information with Server Control. When activated, it allows the use of the actual user name for auditing in PAM Server Control.</p> <p>For more information, see <a href="#">Configure Login Integration for a Server Control Endpoint</a>.</p>



## Install And Configure PAM SC Utility Appliances

The following topics provide end-to-end instructions for installing and configuring PAM SC Utility Appliances (which replace Distribution Servers in the PAM integration).

- [License PAM To Support Server Control](#)
- [Download and Deploy a New Utility Appliance](#)
- [Add Utility Appliances to an Existing Environment](#)
- [Utility Appliance Ports for Network Connectivity](#)
- [Configure PAM to Communicate with Utility Appliances](#)
- [License PAM To Support Server Control](#)
- [View Utility Group Status](#)

### License PAM To Support Server Control

This procedure describes how to license PAM to support Server Control.

#### Follow these steps:

1. Log in into the PAM UI ([https://pam\\_server\\_address/cspm/home](https://pam_server_address/cspm/home)).
2. If you have not already done so, do the following tasks:
  - a. Accept the terms and conditions.
  - b. Log in as super with the default local password.
  - c. Change the default local password.
3. Select **Configuration, Licensing**
4. Copy the Hardware ID.
5. if you do not already have one, obtain a license file with Server Control support from Broadcom support.
6. Do the following tasks to install the license file:
  - a. Navigate to the **Configuration, Licensing** page and select the **Install New License** tab.
  - b. Choose the appropriate license file and select **Upload file**.
  - c. Verify the new license and select **Save New License**.

### Download and Deploy a New Utility Appliance

Use this procedure to download and deploy a new Server Control Utility Appliance VMWare OVA for major (X.x) release.

#### Follow these steps:

1. Download the Utility Appliance software from the Broadcom Support site. For more information, see [Download PAM Installation Media](#).
2. Import the PAM Utility Appliance OVA into VMWare or a VMWare-compatible infrastructure.
3. Read and accept the license.
4. Select **Properties** of the imported OVA.
  - a. Set network and disk specifications as required.
  - b. Take a snapshot of the image before starting.
5. Start the VM.

#### TIP

The Utility Appliance can take several minutes to load upon its initial boot. The Blue Console screen appears in VMWare when the initial deployment process is complete and the Utility Appliance VM is ready to use.

6. Select **Network Interfaces** and take note of the IP address that is assigned to the Utility Appliance VM.
7. Stop the Utility Appliance VM and do the following steps before configuring the Utility Appliance in PAM:
  - a. Take a snapshot of the Utility Appliance VM.

- b. Clone the Utility Appliance VM. The Utility Appliance is shipped with a default SSH key that is known to PAM. Once the Utility Appliance is added to PAM, that key is rotated and cloning of that Utility Appliance is no longer recommended.

## Add Utility Appliances to an Existing Environment

This content describes how to add Utility Appliances to an existing PAM SC environment.

### Follow these steps:

1. [Deploy the new Utility Appliances.](#)
2. [Add the Utility Appliances to PAM.](#)
3. [Add the Utility Appliances to a Utility Group.](#)
4. [Apply the update patches deployed on the existing Utility Appliances to the new Utility Appliances.](#)

## Utility Appliance Ports for Network Connectivity

This content lists the default ports that must be open in the firewall of the Utility Appliance (UA) host for it to establish network connectivity to the PAM server and endpoint agents.

### Assign IP Addresses for the Utility Appliance

Before you configure your network, assign and allocate IP addresses for each Utility Appliance.

### Review Port Assignments

The following table lists the ports required to be open in the host instance firewall for connectivity between .

Port(s)	Protocol	Source	Destination	Notes
443	TCP	UA	PAM	Required in case of PAM cluster primary site failover. Ports need to be open between UAs and <i>all</i> PAM nodes at the primary site and all secondary sites.
22	TCP	PAM	UA	Required for PAM to securely manage Utility Appliances using SSH.
6443	TCP/SSL	PAM	UA	Required for PAM to manage micro services running inside Utility Appliance over TLS.
2379-2380	TCP	PAM	UA	Required to manage the Kubernetes cluster. Ports need to be open between UAs and all the PAM nodes in the Primary Site and all Secondary Sites (in case of primary failover)
2379-2380	TCP	UA	UA	Ports need to be open between all UAs within the same utility group. For example, if you have a utility group named "UG_US_East" containing UAs named "UA1," "UA2," and "UA3" these ports need to be open between UA1, UA2, and UA3.
10250	TCP	PAM	UA	Required to manage the Kubernetes cluster.
10259	TCP	PAM	UA	Required to manage the Kubernetes cluster.
10259	TCP	UA	UA	Required to manage the Kubernetes cluster.
10257	TCP	PAM	UA	Required to manage the Kubernetes cluster.
10255	TCP	PAM	UA	Required to manage the Kubernetes cluster.

28089	TCP	PAM	UA	PAM to A2A; but no filtering on PAM IPs open to all. PAM and A2A have mutual handshake.
5249	TCP	SC Agent	UA	Required by PAM to manage Server Control policies on SC Agents when SSL mode is enabled.
8891	TCP	SC Agent	UA	Required by PAM to manage Server Control policies on SC Agents when SSL mode is not enabled.
61616	TCP/SSL	SC Agent	UA	Required by SC Agents, PUPM Agents, Report Agent, and UNAB Agents running on Endpoint to transfer messages to and from the Utility Appliance
8161	TCP/SSL	Browser	UA	Required only when debugging and diagnosing activemq message queues, if necessary. Otherwise, you can leave it closed.
9095	TCP/SSL	PAM	UA	Required for UNAB policy management and login integration.
7243	TCP/SSL	SC Agent	UA	Required for legacy v12.x PAM SC agents that require Report Agent and UNAB functionality

## Configure PAM to Communicate with Utility Appliances

Distribution Server software is now hosted on Utility Appliances, which are virtual machine instances that you download and deploy. This content describes how to configure PAM to communicate with Utility Appliances by creating corresponding devices and placing them in device groups.

### NOTE

For information about downloading and deploying Utility Appliances, see [Download and Deploy a New Utility Appliance](#).

- [Configure PAM Devices for Utility Appliances](#)
- [Add Utility Appliance Devices to Utility Groups](#)
- [Locate Utility Appliance Devices and Utility Groups](#)
- [Export and Import PAM SC Utility Appliance Devices and Device Groups](#)
- [Replace a Utility Appliance](#)

## Configure PAM Devices for Utility Appliances

### NOTE

#### Prerequisites:

- A PAM server that is licensed for Server Control
- At least one deployed and running Utility Appliance

To configure PAM to communicate with a Utility Appliance VM, create a corresponding Utility Appliance device. PAM then automatically creates and configures all the other objects that are required to enable integration of the Utility Appliance.

### NOTE

This procedure describes how to add Utility Appliance using the PAM UI. You can also add devices using the External API or by uploading an appropriately formatted CSV file.

#### Follow these steps:

1. Navigate to the **Devices, Manage Devices** screen.
2. Select **Add** to create a new device for your utility appliance.  
The **Add Device** dialog opens.

3. Complete the following fields on the **Basic Info** tab.
  - **Name:** Specify the Utility Appliance name to be displayed on the Access page. You can enter double-byte characters.
  - **Address:** Enter the IP address or FQDN of the Utility Appliance.
  - **Operating System:** Select **Utility Appliance**.
4. Select **OK**.
5. Wait while PAM completes configuration of the Utility Appliance, which can take several minutes.

**NOTE**

When configuration is complete, PAM rotates the Utility Appliance target account private and public keys. Both keys are then rotated every time that someone logs into the Utility Appliance.

**CAUTION**

Do not change any of the properties that PAM configures; doing so breaks the integration of the PAM server and the Utility Appliance.

- Device configuration fields and options:

**Basic Info** tab:

- **Device Type:** Sets the following options:
- **Access:** Designates the Utility Appliance as a potential endpoint for access management
- **Password Management:** Designates the Utility Appliance as a target device for credential management
- **A2A:** Sets this option to provide A2A credential management for the Utility Appliance:
  - **Description 1:** Describes the device (specifically *Utility\_Appliance*)
  - **Active:** Allows the A2A Client to receive credentials

**Access Method** tab: Adds the **SSH** access method and configures it for communication with the Utility Appliance

- A corresponding target application with the following properties:
  - **Host Name:** The IP address or FQDN of the Utility Appliance device
  - **Device Name:** The name of the Utility Appliance device
  - **Application Name:** "Utility Appliance Application"
  - **Application Type:** UNIX
- A corresponding target account with the following properties:
  - **Host Name:** The IP address or FQDN of the Utility Appliance device
  - **Device Name:** The name of the Utility Appliance device
  - **Application Name:** "Utility Appliance Application"
  - **Account Name:** "root"
  - **Password View Policy:** The UtilityAppliancePVP policy rotates the Utility Appliance credentials at the end of each connection.
  - **Protocol:** SSH-2 Public Key Authentication"
  - **Private Key:** A generated private key
  - **Public Key:** A generated public key

**TIP**

**Troubleshooting Tip:** If a message appears stating that the device was defaulted to a Linux OS Type, there was likely a communication error. Information can be found on the **Sessions Logs** screen.

## Add Utility Appliance Devices to Utility Groups

A Utility Group consists of a set of Utility Appliance devices that are associated together in a cluster. An end user can assign and deploy policies on:

- A single Utility Appliance device
- Different Utility Groups
- A combination of a Utility Appliance device and a Utility group

Note the following guidance:

- Each Utility Appliance can only be assigned to one Utility Group at any time.
- The Utility Appliances grouped in a Utility Group run orchestration software to coordinate with each other. As such, these Utility Appliances should be co-located within the same network region, firewalled area, or Datacenter.
- PAM is unable to determine the location of Utility Appliances in relation to each other. As a result, you must know and set up the information in PAM appropriately.

To create a Utility Group, add Utility Appliance devices to Utility Groups with a provision type of `Utility Group` to make them operational.

#### NOTE

Each Utility device can belong to only one Utility Group.

**To add Utility Appliance devices to Utility Groups, follow these steps:**

1. Navigate to **Devices, Manage Device Groups**.
2. Select **Add** to create a new device group for your Utility Appliances. The **Add Device Group** dialog opens.
3. Enter a name for the Utility Group in the **Name** field.
4. Select **Utility Group** from the **Provision Type** drop-down.
5. On the **Devices** tab, move the desired Utility Appliance devices from the **Available Devices** list to the **Selected Devices** column.
6. Select **OK**.

PAM creates a cluster from the Utility Appliances in a Utility Group, starting the Distribution Server software on the Utility Appliances, which then start communicating with PAM.

To verify that the operation was successful, navigate to **Credentials, Manage A2A, A2A Clients** and check the status indicator beside the listed Utility Appliances.

#### IMPORTANT

When updating a Utility Group, *do not* remove *all* current members and add a new member or members in a single update operation.

Instead, use multiple updates as shown in the following procedure:

1. Remove all members from the Utility Group and commit the change.
2. Add the required new members to the Utility Group and commit the change.

## Locate Utility Appliance Devices and Utility Groups

This content describes how to locate configured Utility Appliance Devices and Utility Groups in the PAM UI.

### Locate Utility Appliance Devices

Use this procedure to locate all configured Utility Appliance devices.

**Follow these steps:**

1. Navigate to the **Devices, Manage Devices** screen.
2. Open the **Column** drop-down and select **Operating System**.
3. Select the **Value** field. The **Select Operating System** dialog appears.
4. If any Utility Appliances exist, `Utility Appliance` appears in the **Available Operating System** column.
5. Move the `Utility Appliance` entry to the **Selected Operating System** column.

6. Select **OK**.
7. Select **Filter**.

### **Locate Utility Groups**

Use this procedure to locate all configured Utility Groups.

#### **Follow these steps:**

1. Navigate to the **Devices, Manage Device Groups** screen.
2. Open the **Column** drop-down and select **Provision Type**.
3. Select the **Value** field. The **Select Provision Type** dialog appears.
4. If any Utility Groups exist, *Utility Group* appears in the **Available Provision Type** column.
5. Move the *Utility Group* entry to the **Selected Provision Type** column.
6. Select **OK**.
7. Select **Filter**.

## **Export and Import PAM SC Utility Appliance Devices and Device Groups**

As a Privileged Access Manager administrator, you can export a list of Utility Appliance devices or Utility Appliance device groups in CSV format. These files can optionally be modified and later be imported, preventing the need to add the devices or groups individually.

### **IMPORTANT**

To use the Import/Export functions with Internet Explorer (IE), verify that the following security settings are configured:

1. Open Internet Explorer.
2. Select **Tools, Internet Options**.
3. In the Internet Options pop-up window, select the **Security** tab.
4. Select the slider zone
5. Select **Custom level**. Scroll to **Downloads**. For **File download**, select the **Enable** option.
6. Select **OK** to save changes.

### **Export Utility Appliance Devices to a CSV file**

Use this procedure to download a CSV list of all configured Utility Appliance devices.

#### **Follow these steps:**

1. Navigate to the **Devices, Manage Devices** screen.
2. Open the **Column** drop-down and select **Operating System**.
3. Select the **Value** field. The **Select Operating System** dialog appears.
4. If any Utility Appliances exist, *Utility Appliance* appears in the **Available Operating System** column.
5. Move the *Utility Appliance* entry to the **Selected Operating System** column.
6. Select **OK**.
7. Select **Filter**.
8. Select **Import/Export**.
9. On the **Import/Export** dialog that opens, select **Export Devices**. This exported file can optionally be used to make a revised version and then imported back into Privileged Access Manager.

### **Export Utility Appliance Device Groups to a CSV file**

Use this procedure to download a CSV list of all configured Utility Appliance device groups.

#### **Follow these steps:**

1. Navigate to the **Devices, Manage Device Groups** screen.
2. Open the **Column** drop-down and select **Provision Type**.
3. Select the **Value** field. The **Select Provision Type** dialog appears.
4. If any Utility Groups exist, **Utility Group** appears in the **Available Provision Type** column.
5. Move the **Utility Group** entry to the **Selected Provision Type** column.
6. Select **OK**.
7. Select **Filter**.
8. Select **Import/Export**.
9. On the **Import/Export** dialog that opens, select **Export Devices**. This exported file can optionally be used to make a revised version and then imported back into Privileged Access Manager.

### **Import Utility Appliance Devices or Utility Appliance Device Groups from a Previously Exported CSV file**

This procedure describes how to import Utility Appliance devices or device groups from an exported CSV file.

#### **Follow these steps:**

1. Go to **Devices, Manage Devices**.
2. Select **Import/Export**.  
The **Import/Export Devices** window appears.
3. In the **Import/Export Devices** window, select **Choose File** to select the file, and select **Import Devices**.  
The content of the file is added to the existing device database. The new content does not replace the current database.
4. Navigate to **Devices, Manage Devices**, and confirm that the import was successful by inspecting the device list.

### **Replace a Utility Appliance**

This content describes how to replace a Utility Appliance with another, for example, to move the Utility Appliance to a more powerful server.

#### **Follow these steps:**

1. Navigate to the **Devices, Manage Device Groups** screen.
2. Select the Utility Group that contains the Utility Appliance that you want to replace and select the **Update** button.
3. Remove the Utility Appliance from the Utility Group by moving it from the **Selected Devices** column to the **Available Devices** column.
4. Select **OK**.
5. Navigate to the **Devices, Manage Devices** screen.
6. Select the Utility Appliance that is being replaced and select the **Delete** button.
7. [Download and deploy a new Utility Appliance](#).
8. [Configure the new Utility Appliance device](#) with the same IP address as the one that you deleted.

#### **IMPORTANT**

Because Endpoints are registered to the Utility Appliance by IP address, it is important to assign the new Utility Appliance the same IP address as the old one that it is replacing.

9. [Add the new Utility Appliance to the Utility Group](#) from which you removed the old one.

## Deploy and Manage Utility Appliance Update Patches

Utility Appliance update patches provide updates for new PAM releases, periodic fixes, new functionality, or both. This content describes how to deploy and manage Utility Appliance update service patches from the PAM UI.

### IMPORTANT

You must apply the same patch versions to all the active Utility Appliances (that is, members of Utility Groups) in your environment.

### Deploy a Utility Appliance Service Patch

Use the following procedure to deploy a Utility Appliance patch to all active Utility Appliances.

#### Follow these steps:

1. Download the required patch archive (for example, `pam-utility-appliance-1.0.0.6.p.zip`) from [Broadcom Support](#) and extract its contents (a `.bin` and a `.sha256` file) to a local drive.

### IMPORTANT

Do not discard downloaded patch files. If you later add Utility Appliances to a new or existing Utility Group, these patch files are required to reupload and restage each patch (unless you must change the existing Patch Level).

2. Open the PAM UI and navigate to **Configuration, Utility, Patches, Utility Appliance Patches**.
3. On the **Available Patches** tab, select **Upload**.
4. On the dialog that opens, select **Choose File**, locate, and select the patch executable (`.bin`) file, and then select **Upload**.
5. Verify that the file information is correct and select **Save**.  
The patch is uploaded to the PAM server and the service updates that it contains are added to the list of patches that are available to stage.
6. Do the following steps for each listed Utility Appliance service patch.
  - a. Select the patch and select **Stage**.
  - b. On the dialog that opens, verify that the patch information is correct and select **Yes**.

### NOTE

Take a note of the name of each patch that you stage to identify which services to update in Step 7.

7. Select the **Patch Level** tab and do the following steps to update each service that you staged in Step 6:
  - a. Select the appropriate entry from the following list of displayed services and select **Update**.
    - `pam-dh`
    - `pam-loginintegration`
    - `pam-activemq`
    - `pam-config`
    - `pam-eventforwarder`
    - `reloader`
    - `pam-a2a`
    - `activemq-config`
    - `pam-policyorchestrator`
  - b. On the dialog that opens, select the new patch version from the drop-down box and select **OK**. The version number of the patch may be later or earlier than your existing version number.

### NOTE

If no patch is staged for this service, the drop-down box is empty, and you cannot continue.

The service is updated on each Utility Appliance in the Utility Group and the new patch version is displayed in the patch level list.



## **Delete a Utility Appliance Patch**

Use this procedure to delete a patch that has not yet been staged or deployed.

### **NOTE**

You cannot delete a patch that has been staged or deployed. However, you can change which patch is deployed to your Utility Appliance on the **Patch Level** tab.

### **Follow these steps:**

1. On the **Available Patches** tab, select the patch that you want to delete. You cannot delete a patch that has been staged or deployed. However, you can change which patch is deployed to your Utility Appliance on the **Patch Level** tab.
2. Select **Delete**. You can only delete a patch that has not yet been staged.  
Once the patch has been deleted, it is removed from the list on this tab.

## **View information About Deployed Patches**

Select the **Patch Activity** tab to view the following information about each deployed patch:

- **Service:** To which service the patch was deployed.
- **From Version:** The patch level before the current patch was deployed.
- **To Version:** The patch level after the current patch was deployed.
- **Start Time:** When the current patch was deployed.
- **User:** The system administrator that deployed the patch.
- **Notes:** Any additional information about the patch that is provided with the patch. This field may be blank if no information is included with the patch.

Select a service in the list and then select **View** to see the following detailed information about a deployed patch:

- **Utility Group:** The name of the utility group to which this service belongs.
- **Devices Complete:** The number of devices that are in the utility group and to which the update has been deployed.
- **Status:** The progress of the latest update.
- **Last Status Time:** When the utility group was last updated.
- **Notes:** Any additional information about the service update that is provided with the patch. This field may be blank if no information about the service update is included with the patch.

## **View Utility Group Status**

The Utility Group Status panel provides comprehensive status information about the Utility Appliances that are configured in Utility Groups in your environment.

### **Access the Utility Group Status Panel**

To access the Utility Group Status panel, navigate to **Configuration,Utility, Status** in the PAM UI.

The **Utility Group Status** panel lists all the Utility Groups in your environment. Select the **Name** or **Description** column headers to sort the list.

### **Obtain the Status of a Utility Group**

To obtain the status of a listed Utility Group, double-click that group or select the entry and select the **View** button in the top right-hand corner.

The **View Utility Group** dialog opens, displaying the **Devices** tab.

## View Utility Group Tab Descriptions

The **View Utility Group** dialog provides comprehensive information about the corresponding Utility Group in the following tabs:

### Basic Info Tab

Provides the Utility Group name and description

### Devices Tab

The **Devices** tab provides information about the status of each Utility Appliance in the Utility Group and the services running on it.

## View UG-45

Basic Info   **Devices**   Services   Config Maps

All Services

10.17.45.142		✓	i	
pam-a2a	4.0.0.29	✓	i	
pam-activemq	4.0.0.164	✓	i	
pam-dh	4.0.0.164	✓	i	
pam-loginintegration	4.0.0.164	✓	i	
pam-policyorchestrator	4.0.0.164	✓	i	
10.17.45.179		✓	i	
pam-a2a	4.0.0.29	✓	i	
pam-activemq	4.0.0.164	✓	i	
pam-dh	4.0.0.164	✓	i	
pam-loginintegration	4.0.0.164	✓	i	
pam-policyorchestrator	4.0.0.164	✓	i	
reloader	4.0.0.29	✓	i	
10.17.45.238		✓	i	
pam-a2a	4.0.0.29	✓	i	
pam-activemq	4.0.0.164	✓	i	
pam-dh	4.0.0.164	✓	i	

Close

**NOTE**

The services are [explained in a table](#) later in this topic.

The top row of the Devices tab provides controls that allow you to:

- Filter on a specific service name.
- Download a JSON file containing comprehensive information about the Utility Group and its members.
- Expand or collapse all entries in the table.
- Recycle all Utility Appliance services. Recycling a service kills it, forcing PAM SC to reschedule the service on the same or another host (depending on its configuration).

**NOTE**

Recycling can be useful when services do not start correctly, clearing the issue and allowing the services to start successfully.




Status Icons for **Devices** and **Service** tabs:

Each row in the following table provides status information and options for a Utility Appliance or a service running on a Utility Appliance.

Status Icon	Meaning for a Utility Appliance	Meaning for a Service
Green check mark	Utility Appliance is healthy to run services. No Disk, RAM, CPU pressure.	The service is deployed and running. (This status does not report the health of the service functionality – only that it is running.)
Yellow bell	N/A	Attempt to deploy the service on this Utility Appliance was made, but the service does not start.
Red stop sign	Utility Appliance is not reachable or not ready to run services on this device.	Either the Utility Appliance is unreachable (see the previous row) or the service cannot run for some other reason.

Functional Icons for **Devices** and **Service** tabs:

The following table describes the status and functional icons that appear beside each entry on the **Devices** and **Services** tabs:

Icon	Meaning
Information icon (  )	Returns detailed information about the associated Utility Appliance or service.
View service logs icon (  )	Returns the logfile for the associated service.
Recycle service icon (  )	Kills the service, forcing PAM SC to reschedule the service on the same or another host (depending on its configuration). Recycle can be useful when the service did not start correctly. Recycling can clear the issue and result in the service starting successfully.

**Services Tab**

The **Services** tab provides an alternative view of devices and services, grouping the list by service and showing the utility appliances on which each service is running.

## View UG-45



Basic Info   Devices <b>Services</b> Config Maps			
<div> <div>+</div> <div>-</div> <div>↺</div> </div>			
- pam-a2a		✓ ..	↺
10.17.45.142	4.0.0.29	✓ .. ⓘ 📄	↺
10.17.45.179	4.0.0.29	✓ .. ⓘ 📄	↺
10.17.45.238	4.0.0.29	✓ .. ⓘ 📄	↺
- pam-activemq		✓ ..	↺
10.17.45.142	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.179	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.238	4.0.0.164	✓ .. ⓘ 📄	↺
- pam-dh		✓ ..	↺
10.17.45.142	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.179	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.238	4.0.0.164	✓ .. ⓘ 📄	↺
- pam-loginintegration		✓ ..	↺
10.17.45.142	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.179	4.0.0.164	✓ .. ⓘ 📄	↺
10.17.45.238	4.0.0.164	✓ .. ⓘ 📄	↺
- pam-policyorchestrator		✓ ..	↺

Close

(The Services tab uses the same status and functional icons as the Devices tab described previously.)

The following table describes all available services:

Service Name	Description	
pam-config	Sends the PAM configuration map to the Utility Group.	Changes when the
reloader	A utility within the Utility Group that watches for configuration changes. The reloader utility knows which other services to recycle when a specific configuration is changed.	Only one is needed per Appliance.
pam-a2a	Communicates with PAM to service Utility Appliance information that is stored when a Policy assigned or finalized.	One required for each

Service Name	Description	
pam-policy-orchestrator	Communicates between the Utility Appliance and PAM A2A. Facilitates device registration for Server Control, Login Integration, and UNAB.	One required for e
pam-dh	Allows Server Control endpoints to communicate with the DH for policy information.	One required for e
activemq-config	Configuration values that are used by ActiveMQ and other dependent services like eventforwarder.	Updates if the PA
pam-activemq	Endpoints connect to ActiveMQ for Login Integration, UNAB, and Event Forwarder.	One required for e
pam-eventforwarder	Syslog/Splunk consumer from ActiveMQ to an external server	If the PAM Syslog on each Utility Ap
pam-loginintegration	Service that listens for calls from PAM to process a login integration transaction	One required for e
pam-tibco	Service required to support the optional Tibco component (which is available as a patch that can be applied from <b>Configuration, Utility, Patches.</b> )	If the Tibco patch once per Utility Ap

### Config Map Tab

The **Config Map** tab displays the values of *Config Map* objects (key-value pairs) which determine the behavior of the Utility Appliances in the Utility Group.

## View pam.utilityappliance.group



### Basic Info Devices Services Config Maps

•			+	-	↺
Configuration	Key	Value			
- activemq-config	tibco-enabled	true			
	activemq-pwd-alias	activemq-pwd-alias1619098036			
	evenforwarder-enabled	true			
- pam-config	pamurl	10.17.45.16			
- syslog-config	syslog	syslog=TENANT;;TENANT=1;ENABLE=TRUE;FORMAT=AUDIT_FORMAT_CEF;TENANT_TYPE=AUDIT_SYSTE M_SIEM;HOST=10.17.47.16:6131			

### NOTE

The data on the Config Map tab is read-only. Select the links in the following descriptions for information about how to change the settings.

- **activemq-config**: Displays the following configuration information that is related to ActiveMQ and other dependent components in the utility group:
  - [Whether the Utility Group is TIBCO-enabled \(to support older PIM agents\)](#)
  - [ActiveMQ password changes](#)
  - [Whether the Event Forwarder is enabled](#)
- **pam-config**: [The VIP address of the cluster](#).
- **syslog-config**: [Syslog information](#) that is used by the Event Forwarder component (only displayed when eventforwarder is enabled).

#### NOTE

When the value of any Config Map object is updated, PAM recycles all services that use that value running on Utility Group members. Therefore, services on Utility Appliances always run with the latest configuration information.

## Migrate From PIM or PAM SC to PAM

This section describes the process of migrating from Privileged Identity Manager or Privileged Access Manager Server Control to Privileged Access Manager.

**Use the table of contents to access the topics in this section.**

### Migrate Policy Management Data

The procedures in this section describe how to migrate Policy Management Data.

**Use the table of contents to access the topics in this section.**

### Prepare to Migrate to PAM

This section contains the prerequisite steps and preparatory procedures for migration from PIM or PAM SC to PAM.

**Use the table of contents to access the topics that described these prerequisite steps and preparatory procedures.**

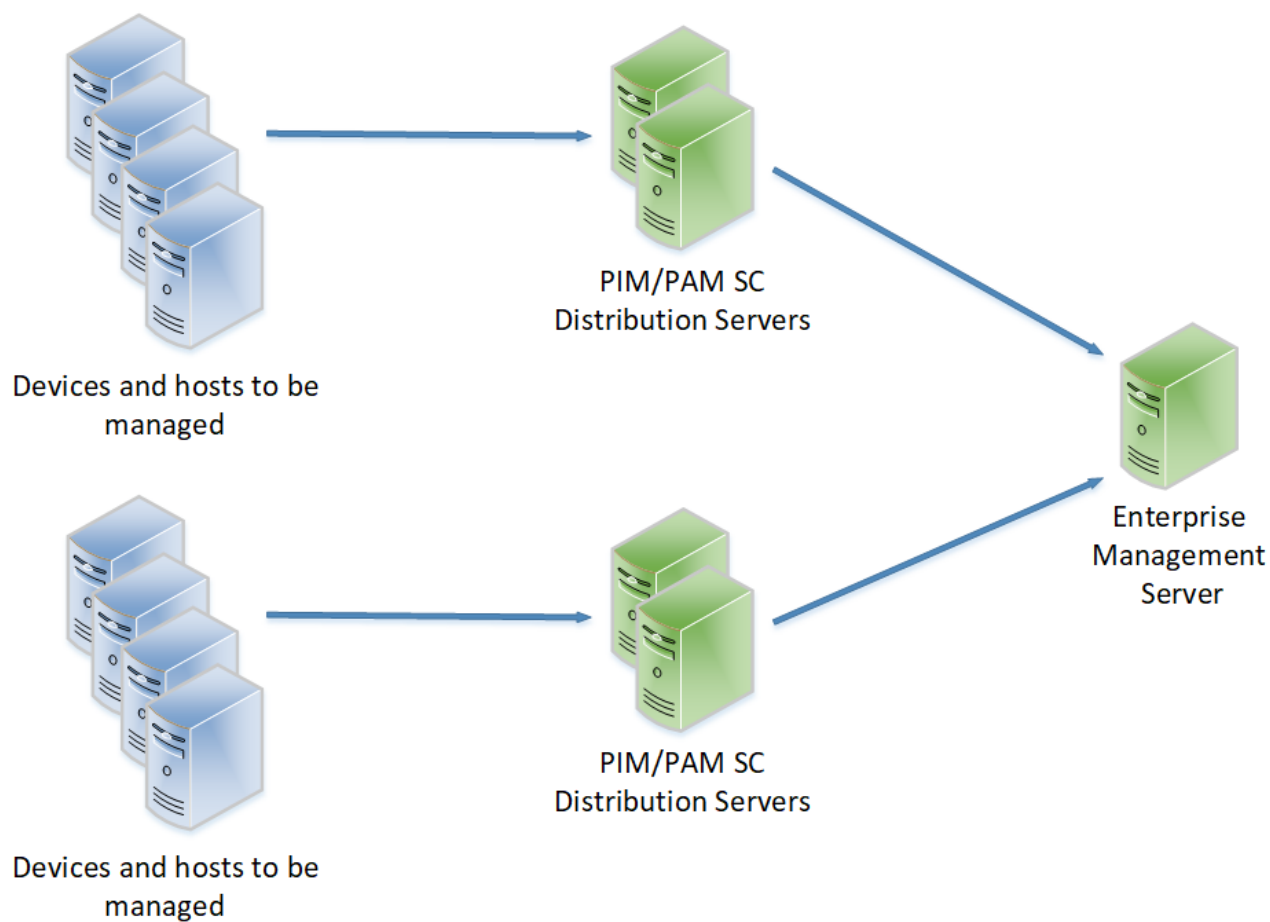
### Deployment Architecture Changes During Migration

This content illustrates how the architecture of a PIM or PAM SC deployment changes during the migration process. Review this content before starting your migration.

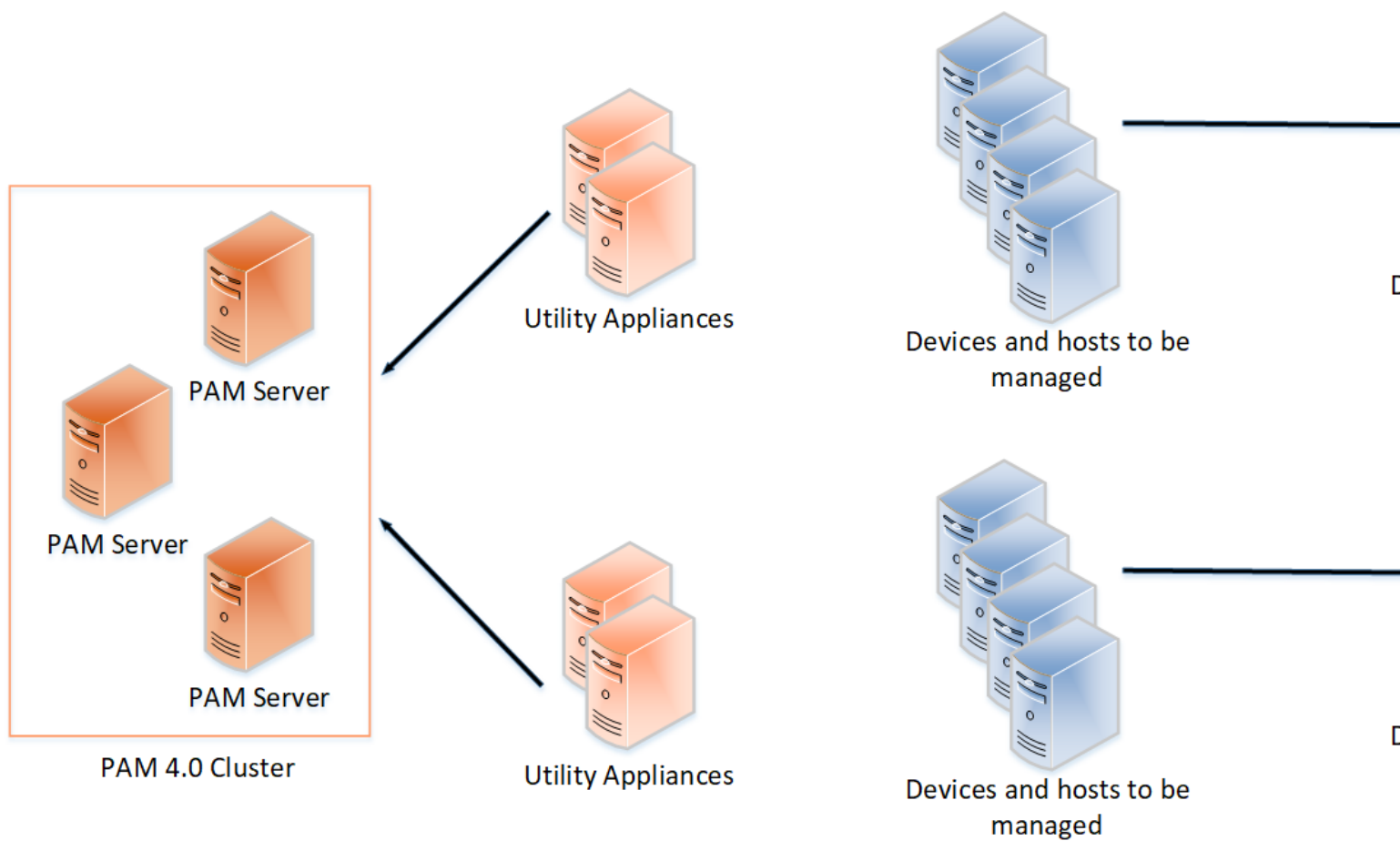
#### For PIM and PAM SC Deployments

This section illustrates how your deployment architecture changes during the migration process.

**Pre-migration:** Existing PIM or PAM SC logical deployment. PAM 4.0 is not yet deployed.

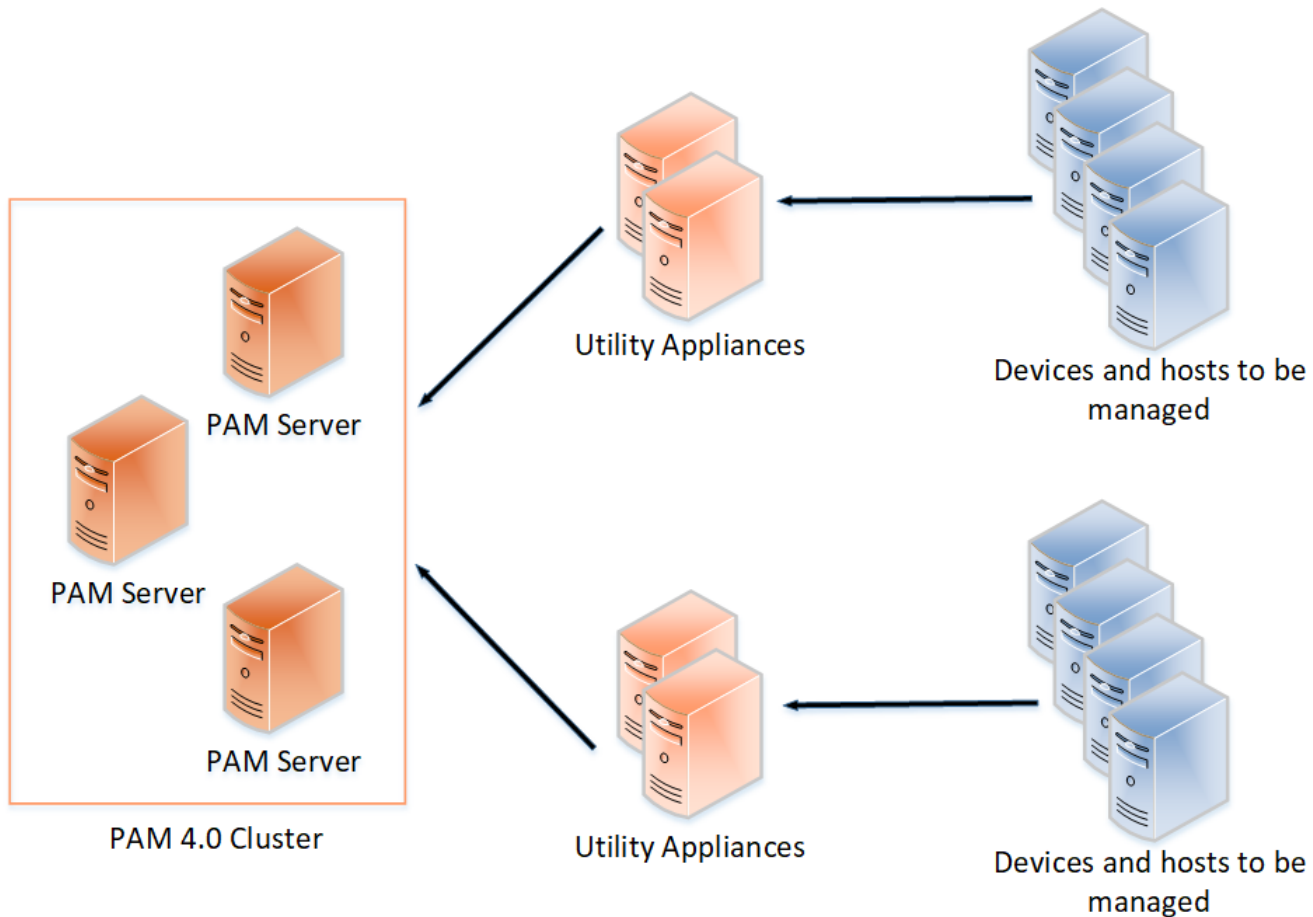


**Stage 1:** Deploy PAM 4.0 and Utility Appliances, but devices and endpoints are still managed by PIM or PAM SC.



**Stage 2:** Devices transition from management by the Distribution Server to management by the Utility Appliance.





### **For PAM-Only Deployments Adding Server Control Functionality**

If you currently only have a PAM deployment, you need only review the left side of Stage 3 and then complete the following procedures:

- Deploy Utility Appliances.
- Install Endpoint Agents on the devices.
- Configure the Endpoint Agents to point to a Utility Appliance.

### **Gather required information from the PIM or PAM SC ENTM Server**

This content describes how to gather required information from the PIM or PAM SC ENTM server.

#### **Follow these steps:**

1. Log on to the PIM or PAM SC ENTM server.
2. Take a note of policies, devices, device groups, deployments, and audit information.
3. Navigate to **Worldview, Hosts** and verify that at least two endpoints are configured against ENTM. Refer to the given environment details and provide proper search criteria in the Host Name.
4. Check the pre-migrated data like **hosts, policies, and host groups**

## Deploy or Upgrade an Existing PAM Deployment to 4.x

Deploy and configure a new 4.x PAM environment or upgrade an existing pre-4.0 PAM environment to PAM 4.0.

For more information, see the following resources:

- If you have no existing PAM environment, see [Deploying](#).
- If you have an existing pre-4.0 PAM environment, see [Upgrading](#).

## Migrate Data from PIM or PAM SC to PAM on Windows

Complete the following procedures to migrate your data from PIM or PAM SC to PAM on Windows.

### Prepare to Install the Migration Utility

1. Verify that you have PAM version 4.0 or later.
2. Log in to the PAM UI.
3. Complete the following steps to configure API keys for the user:
  - a. Select **Users, Manage Users**.
  - b. Select the Super User for which you want to enable the API keys and select **Update**.
  - c. On the **API Keys** tab, add an API key name.
  - d. Select **OK**.
4. Complete the following steps to configure API keys (password) for the user:
  - a. Select **Credentials, Manage Targets, Accounts**.
  - b. Select the API key name that you created in the previous step and select **Update**.
  - c. Set a password for the API key and select **OK**.
5. If your PIM or PAM SC environment includes UNAB policy data, do the following steps to configure and import groups and users from an LDAP server:
  - a. Do the following steps to configure a device and target application for the LDAP server:
    - a. Navigate to **Devices, Manage Devices** and select the **Add** button.
    - b. Provide the details of the LDAP server and verify that the **Password Management** device type option is set.
    - c. Select the **Save and Add Target Applications** button.
    - d. Enter an **Application Name** and select **Active Directory** from the **Application Type** drop-down menu.
    - e. Select the **Active Directory** tab that appears, provide the **Domain Name** and select the **OK** button to save your changes.
  - b. Do the following steps to create a target account to manage the Active Directory target application that you created:
    - a. Navigate to **Credentials, Manage Targets, Accounts**.
    - b. Select the **Add** button.
    - c. Enter the administrator **Account Name** and **Password**.
    - d. Enter or select the **Application Name** of the target application that you created. The **Host Name** and **Device Name** fields are populated and an **Active Directory** tab appears.
    - e. Select the **Active Directory** tab and enter the appropriate **Distinguished Name**. For example:  
CN=Administrator,CN=Users,DC=warriors,DC=com.
  - c. Navigate to **Configuration, 3rd Party, LDAP**, select the **Add** button, and enter the LDAP domain information.
  - d. Connect to PAM using the PAM client and import the groups and users (required for UNAB login policies).
6. Navigate to the PAM SC install location, C:\Program Files\CA\AccessControlServer\APMS\AccessControl\bin.
7. If you already have Server Control policies or device groups that are defined in PAM with the same names as policies or device groups that are defined in PIM/PAM SC, do one of the following steps to avoid migration errors:

- To retain the Server Control policies or device groups that are defined in PIM/PAM SC, delete the similarly named objects from PAM.
  - To retain existing Server Control policies or device groups that are defined in PAM, delete the similarly named objects from PIM/PAM.
8. Turn off access control on the PAM SC Server using the following command:
- ```
secons -s
```

### **Install the Migration Utility**

1. On the PAM SC server, locate and launch the Migration Utility installer, `MigrationUtility.exe`.
2. When the installer opens, follow the prompts:
  - a. On the **Choose Install Folder** panel, specify an install location.
  - b. On the **Pre Check Migration or Migration** panel do one of the following steps:
    - To perform end-to-end migration into PAM (Data Extraction, Validation, and Import data in to PAM), select **Migration**.
    - To perform only data extraction and validation to prepare the data for import in to PAM, select **Pre Check Migration**.
  - c. . On the **Launch Migration Utility** panel, select the **Launch Migration Utility** option if you want the installer to launch the Migration Utility directly after installation.
  - d. On the **Installation Complete** panel, select **Done**.

### **Run the Migration Utility**

This procedure describes how to run the migration utility to move your data from PIM/PAM SC to PAM.

#### **Follow these steps:**

1. If you set the **Launch Migration Utility** option during installation, the **PIM to PAM Migration Utility** starts. If not, navigate to `Migration_Installation_location/bin` and start **Migration.bat** to launch the utility manually. The utility opens at a home panel that displays all the steps that are involved in the migration process.
2. Specify the **DMS location**.  
The default values for PIM 12.8 and PIM 14 are:
  - Windows: `C:\Program Files\CA\AccessControlServer\APMS\AccessControl\Data\DMS`
  - UNIX: `/opt/CA/AccessControlServer/APMS/AccessControl/Data/DMS`
 The default values for PAM SC 14.0 and PAM SC 14.1 are:
  - Windows: `C:\Program Files\CA\PAMSCServer\APMS\PAMSC\Data\DMS`
  - UNIX: `/opt/CA/PAMSCServer/APMS/PAMSC/Data/DMS`
3. Specify a **Staging directory**, an empty folder where all the PIM/PAM SC data is extracted and stored for processing and validation.
4. Select the **Initialize** button to begin the extraction process. The utility sets up the staging location, and prepares for the data migration.
 

**NOTE**

If you have previously completed some migration on the provided staging location, the utility takes you directly to the phase where you stopped in the previous run. If you want to restart the migration from scratch, create a staging directory.
5. Select **Extract** to extract all the PIM or PAM SC data and deployment records from the ENTM DMS to the specified staging location.  
The live status of the records that are being extracted is shown in the utility.
6. When data extraction is successfully completed, select **Validate**.  
The utility scans all the PIM/PAM SC records, validating and creating relational mapping of the entities to be compatible with PAM. Validation progress is shown on the **Validate Data** page. If errors occur during migration that are

not an issue, select **Ignore Errors** and then select **OK** in the **Confirmation** dialog that appears. If errors that are an issue occur, see [Troubleshoot Orphaned Data, Records, and Validation Errors](#) for information about how to resolve them.

7. When validation is complete, select **Backup** to take a backup of the PAM server. Complete the following fields on the **PAM Server Details** dialog that appears and then select **OK**:

- **PAM Server Address**: The IP address of the PAM server to which the data is to be migrated.
- **API Key**: The complete API Key name that you set previously in these procedures.
- **API Password**: The API Key password that you set previously in these procedures.

**NOTE**

Make a note of the backup file name.

8. Select **Migrate** to initiate the data migration to the PAM server.

Migration progress is shown on the **Migrate Data** page.

During migration, you can take the following steps to verify that the migration is occurring correctly:

- Select **Pause** to verify the migrated data on the PAM Server. Select **Resume** to continue migration or select **Rollback** to restore the PAM database to the premigration state.
- Check the PAM environment in parallel to verify that the data (Devices, Device Groups, Policies, and Deployments) are loading correctly.

9. When the data migration to PAM is completed, select **Finalize** to commit the migration.

10. Select **Exit** to close the Migration Utility.

## **Postmigration Steps**

This procedure describes how to cut over from your existing PIM/PAM SC distribution server to a new Utility Appliance configured in PAM.

### **Follow these steps:**

1. Verify that the data (PIM/PAM SC Policies, Devices, Device Groups, Deployment Audit) is successfully migrated to PAM.
2. Check the **Agent Status** page to verify that the Uninitialized count should be equal to the number of migrated but not initialized devices.
3. Complete the following steps to re-configure PIM/PAM SC devices to communicate with the new PAM Utility Appliance:
  - a. Navigate to the PIM/PAM SC Access Control Server location. For example, `/opt/CA/AccessControlServer/APMS/AccessControl/bin/` or `/opt/CA/PAMSCServer/APMS/PAMSC/bin/`
  - b. Turn on access control on the PIM/PAM SC server.
  - c. Do the following steps to create a PIM/PAM SC policy:
    - a. Open the PIM/PAM SC ENTM user interface.
    - b. Navigate to **Policy Management, Policy, Create Policy**.
    - c. Enter the following commands to run a deployment script that creates a server control policy:
 

```
so dh-
so dh+(DH__@<UtilityServer>)
```
  - d. Assign the previously created policy on PIM/PAMSC devices that you want to configure to communicate with the new PAM Utility Appliance.
  - e. Restart the policyfetcher process on each endpoint (for immediate policy deployment) or wait for a scheduled job to restart the policyfetcher.
4. Complete the following steps to re-configure the PIM/PAM SC UNAB agent to communicate with the new PAM Utility Appliance:
  - a. Open the PIM/PAM SC ENTM user interface.
  - b. Navigate to **Policy Management, UNIX Authentication Broker, Host, Configure a UNAB Host**.
  - c. Select the UNAB device to configure.

- d. In the **Communication** section, select the token **Distribution\_Server** and set the following values:
  - ssl://<Utility Server name or ip address>:61616 for ActiveMQ based devices (for example, pamsc141)
  - ssl://<Utility Server name or ip address>:7243 for Tibco based devices (or example: PIM128)
- e. Submit the config policy.
- f. To configure a group of UNAB devices to work with the new Utility Server, you can choose **Configure a UNAB host group** under **Unix Authentication Broker**.
- g. Go to the UNAB device and set the message queue password:
 

```
<UNAB install dir>/bin/acuxchkey -t -pwd <Communication password of Utility Server>
```

All the PIM/PAM SC migrated devices are now pointed at a PAM Utility Appliance. You can now perform Policy Management activities using the PAM UI.

## Migrate Data from PIM or PAM SC to PAM on Linux

The following procedures describe how to migrate data from PIM or PAM SC to PAM on Linux:

### Prepare to Install the Migration Utility

**Complete the following steps on the PIM SC/PIM server to prepare for migration:**

1. Open a shell window.
2. Navigate to the Access Control Server location. For example, /opt/CA/AccessControlServer/APMS/AccessControl/bin/ or /opt/CA/PAMSCServer/APMS/PAMSC/bin/.
3. Turn off the access control PAM SC/PIM server by entering the following command: `./secons -sk`

**Complete the following steps on the PAM server to prepare for migration:**

1. Log in to the PAM UI.
2. Do the following steps to configure API keys for the user:
  - a. Verify that you are running version 4.0 or later.
  - b. Select **Users, Manage Users**.
  - c. Select the user for which you want to enable the API keys and select **Update**.
  - d. Navigate to the **API keys** tab and add an API key name.
3. Do the following steps to configure API keys (Password) for the user.
  - a. Click **Credentials, Manage Targets, Accounts** in the PAM UI.
  - b. Select the API key name that you created in the previous step, and click **Update**.
  - c. Set a password for the API key and select **OK**.
4. Verify that a Utility Server is installed and configured in PAM.
5. If your PIM or PAM SC environment includes UNAB policy data, do the following steps to configure and import groups and users from an LDAP server:
  - a. Do the following steps to configure a device and target application for the LDAP server:
    - a. Navigate to **Devices, Manage Devices** and select the **Add** button.
    - b. Provide the details of the LDAP server and verify that the **Password Management** device type option is set.
    - c. Select the **Save and Add Target Applications** button.
    - d. Enter an **Application Name** and select **Active Directory** from the **Application Type** drop-down menu.
    - e. Select the **Active Directory** tab that appears, provide the **Domain Name**, and select the **OK** button to save your changes.
  - b. Do the following steps to create a target account to manage the Active Directory target application that you created:
    - a. Navigate to **Credentials, Manage Targets, Accounts**.
    - b. Select the **Add** button.

- c. Enter the administrator **Account Name** and **Password**.
- d. Enter or select the **Application Name** of the target application that you created. The **Host Name** and **Device Name** fields are populated and an **Active Directory** tab appears.
- e. Select the **Active Directory** tab and enter the appropriate **Distinguished Name**. For example:  
CN=Administrator,CN=Users,DC=warriors,DC=com.
- c. Navigate to **Configuration, 3rd Party, LDAP**, select the **Add** button, and enter the LDAP domain information.
- d. Connect to PAM using the PAM client and import the groups and users (required for UNAB login policies).

## **Install the Migration Utility**

Complete the following steps to install the Migration Utility:

1. Open a shell window.
2. Navigate to the location where you downloaded the **MigrationUtility.bin** file.
3. Run the Migration Utility by entering the following command:  
./MigrationUtility.bin  
The Migration Utility installer starts.
4. Follow the prompts, entering the following information when prompted:
  - Enter **Y** to accept the License Agreement.
  - Specify the folder where you want to install the migration utility, then enter it again to confirm the folder.
  - Specify the installed location of the Access Control Server.
  - Enter **2** to install the utility in Migration mode.

The Migration Utility installs.

## **Run the Migration Utility**

Complete the following steps on the PAM SC/PIM server to run the migration utility and complete the migration:

1. Open a shell window.
2. Create a staging directory for all data processing and validation to take place. Create a different staging directory for each installation.  
For example:
  - /opt/CA/AccessControlServer/APMS/AccessControl/policies/DMS\_\_
  - /opt/CA/PAMSCServer/APMS/PAMSC/policies/DMS\_\_
3. Navigate to migration\_utility\_installation\_dir/bin
4. Type the following command to start the Migration Utility: ./Migration.sh  
The Migration Utility starts. The utility displays detailed metrics during each phase of the migration process.
5. Type `start` to initialize the migration process.
6. Verify the displayed Deployment Map Server (DMS) directory location and change it if necessary.
7. Specify the location of the Staging directory that you created earlier in these procedures.
8. Press **Enter**. The utility sets up the staging directory and prepares for data migration.
9. Type `extract` to extract all the PAM SC/PIM data and deployment records from the PAM SC/PIM Access Control Server to the Staging directory that you created earlier in these procedures.  
The live status of the records that are being extracted and the time that is taken are displayed. A progress bar indicates the percentage of records that have been extracted.  
If errors occur during extraction, see [Troubleshoot Orphaned Data, Records, and Validation Errors](#).
10. Upon successful completion of the extraction phase, type `validate` to start the validation phase of the migration process.

In the validation phase, the utility scans the PAM SC/PIM records, validates them, and creates relational mapping of the entities, to be compatible with PAM. A progress bar indicates the percentage of records being validated. If there are errors during Validation, see Validation Errors in [Troubleshoot Orphaned Data, Records, and Validation Errors](#).

- If you selected **Pre Check Migration** during installation of the Migration Utility, only extraction and validation are performed to check the health and readiness of PAMSC/PIM data for migration. No data is migrated. After validation, a success message of *The data is all set for migration to PAM* is displayed and you can quit the Migration Utility.
  - If you selected **Migration** during installation, then proceed with the following steps.
11. When validation is complete, select **Backup** to take a backup of the PAM server. Complete the following fields on the **PAM Server Details** dialog that appears and then select **OK**:
    - **PAM Server IP**: The IP address of the PAM server to which the data is to be migrated.
    - **API Key**: The complete API key name that you set previously in these procedures.
    - **API Password**: The API key password that you set previously in these procedures.

When complete, make a note of the backup filename for future use. The Migration Utility notifies you if PAM is unreachable or if incorrect API Key credentials are provided.
  12. Select **Migrate** to initiate the data migration to the PAM server.  
 Migration begins, and a progress bar indicates the percentage of records migrated.  
 During migration, you can take the following steps to verify that the migration is occurring correctly:
    - Select **Pause** to verify the migrated data on the PAM Server. Select **Resume** to continue migration or select **Rollback** to restore the PAM database to the premigration state.
    - Check the PAM environment in parallel to verify that the data (Devices, Device Groups, Policies, and Deployments) are loading correctly.

Errors, if any, are displayed on the console. See [Troubleshoot Orphaned Data, Records, and Validation Errors](#) for error details.
  13. When the data migration to PAM is completed, select **Finalize** to commit the migration.
  14. Select **Quit** to close the Migration Utility.

### Postmigration Steps

This procedure describes how to cut over from your existing PIM/PAM SC Distribution Server to a new Utility Appliance configured with PAM:

1. Navigate to the PIM/PAM SC Access Control Server location. For example, `/opt/CA/AccessControlServer/APMS/AccessControl/bin/` or `/opt/CA/PAMSCServer/APMS/PAMSC/bin/`.
2. Start access control on the PAM SC/PIM Server by doing the following steps:
  - a. Open two windows under root (superuser) authority.
  - b. In either window, enter the command:  
`seload`  
 Wait while the seload command starts three PIM or PAM SC daemons: Engine, Agent, and Watchdog.
  - c. After you have started the daemons, go to the other window and enter the command:  
`secons -t+ -tv`  
 PIM or PAM SC accumulates a file of messages reporting operating system events. The `secons -tv` command displays the messages on the screen as well.
  - d. In the first window, where you gave the seload command, enter the following command:  
`who`  
 Watch the second window, where PIM or PAM SC is writing the trace messages, to see whether it intercepts the execution of the who command and reports on it. PIM or PAM SC is correctly installed on your system if it reports interception of the who command.
  - e. If you want, enter more commands to see how PIM or PAM SC reacts to them.



The database does not yet contain any rules for blocking access attempts. Nevertheless, PIM or PAM SC monitors the system so that you can see how the system behaves with PIM or PAM SC installed and running, and which events it intercepts.

- f. Shut down the seosd daemon, by entering the following command:

```
secons -s
```

The following message displays on the screen:

```
CA ControlMinder is now DOWN !
```

3. Do the following steps to create a PIM/PAM SC policy:

- a. Open the PIM/PAM SC ENTM user interface.
- b. Navigate to **Policy Management, Policy, Create Policy**.
- c. Enter the following commands to run a deployment script that creates a server control policy:

```
so dh-
```

```
so dh+(DH__@<UtilityServer>)
```

4. Assign the previously created policy on PIM/PAMSC devices that you want to configure to communicate with the new PAM Utility Appliance.
5. Restart the policyfetcher process on each endpoint (for immediate policy deployment) or wait for a scheduled job to restart the policyfetcher.
6. Complete the following steps to re-configure the PIM/PAM SC UNAB agent to communicate with the new PAM Utility Appliance:
  - a. Open the PIM/PAM SC ENTM user interface.
  - b. Navigate to **Policy Management, UNIX Authentication Broker, Host, Configure a UNAB Host**.
  - c. Select the UNAB device to configure.
  - d. Select the **Communication** section, and then select the token "Distribution\_Server" and set the values as follows:
    - ssl://<Utility Server name or ip address>:61616 for ActiveMQ-based devices (for example, pamsc141)
    - ssl://<Utility Server name or ip address>:7243 for Tibco-based devices (for example, PIM128)
  - e. Submit the config policy.
  - f. To configure a group of UNAB devices to work with the new Utility Server, you can choose "Configure a UNAB host group" under Unix Authentication Broker.
  - g. Go to the UNAB device and set the message queue password:

```
<UNAB install dir>/bin/acuxchkey -t -pwd <Communication password of Utility Server>
```

All the PIM/PAM SC migrated devices are now pointed at a PAM Utility Appliance. You can now perform Policy Management activities using the PAM UI.

## How to Change the Migration Utility Timeout Value

By default, the Migration Utility timeout value is set to 120 seconds. You can configure the timeout timeout. For example, to set the timeout to 300 seconds, add the timeout attribute **--http.readtimeout=300** in the corresponding migration batch (for Windows) or sh (for Linux) file. Use the procedure that fits your system:

### Windows

Follow these steps to change the Migration Utility timeout value on Windows systems:

1. Browse to the following location: **<Migration Utility Install Folder>\bin**
2. Open the **Migration.bat** file at this location.
3. Add the timeout attribute to the **JAVA\_EXE** variable, as demonstrated in the following before and after sample:

**Before Modification:**



```
%JAVA_EXE% %JAVA_OPTS% -jar DataProcessor-0.1-SNAPSHOT.jar --install.dir="C:\Program Files
\MigrationUtility" --customer.validation=false --apms.home="C:\Program Files\CA\PAMSCServer\APMS\PAMSC"
%MU_OPTS%
```

#### After Modification:

```
%JAVA_EXE% %JAVA_OPTS% -jar DataProcessor-0.1-SNAPSHOT.jar --install.dir="C:\Program Files
\MigrationUtility" --customer.validation=false --http.readtimeout=300 --apms.home="C:\Program Files\CA
\PAMSCServer\APMS\PAMSC" %MU_OPTS%
```

4. After modifying the **Migration.bat** file, re-run the utility.

## Linux

Follow these steps to change the Migration Utility timeout value on Linux systems:

1. Browse to the following location: **<Migration Utility Install Folder>\bin**
2. Open the **Migration.sh** file at this location.
3. Add the timeout attribute to the **JAVA\_EXE** variable, as demonstrated in the following before and after sample:

#### Before Modification:

```
"$JAVA_EXE" $JAVA_OPTS -jar DataProcessor-0.1-SNAPSHOT.jar --install.dir="/root/MigrationUtility" --
customer.validation=false --apms.home="/opt/CA/PAMSCServer/APMS/PAMSC" $MU_OPTS
```

#### After Modification:

```
"$JAVA_EXE" $JAVA_OPTS -jar DataProcessor-0.1-SNAPSHOT.jar --install.dir="/root/MigrationUtility" --
customer.validation=false --http.readtimeout=300 --apms.home="/opt/CA/PAMSCServer/APMS/PAMSC" $MU_OPTS
```

4. After modifying the **Migration.sh** file, re-run the utility.

## How to Configure the Migration Utility to Work with a Copy of DMS Data

How to configure the Migration Utility to work with a copy of DMS data.

Normally, working with live DMS (Devices, Device Groups, Policies, and Deployments) data requires you to shut down the Access Control Services, which might bring down your production environment for a period of time. However, you can create a process to regularly maintain a *copy* of DMS data so you do not need to shut down the Access Control Services.

This topic shows you how to perform these steps for Windows and Linux.

### How to Configure the Migration Utility to Work with a Copy of DMS Data on Windows

1. Browse to the following location: **<Migration Utility Install Folder>\bin**
2. Open the **Migration.bat** file and update the **CHECK\_AC\_SERVICES** value to **false**, as demonstrated in the following before and after sample:

#### Before Modification:

```
set CHECK_AC_SERVICES=true
set "MU_OPTS=--check.ac.services=%CHECK_AC_SERVICES%"
```

#### After Modification:

```
set CHECK_AC_SERVICES=false
set "MU_OPTS=--check.ac.services=%CHECK_AC_SERVICES%"
```

**NOTE**

If CHECK\_AC\_SERVICES is set to false, then you must also copy the **seos.msg** file. For example: if you have copied DMS\_\_ folder to the C:\backup folder, then you need to copy the seos.msg file **from** C:\Program Files\CA\PAMSCServer\APMS\PAMSC\Data or C:\Program Files\CA\AccessControlServer\APMS\AccessControl\Data **to** c:\backup\DMS\_\_ folder.

3. After modifying the migration batch file, re-run the utility.
4. When prompted for the DMS location, provide the backup folder, that is, either **C:\backup\DMS\_\_** or **/work/backup/DMS\_\_**.

**How to Configure the Migration Utility to Work with a Copy of DMS Data on Linux**

1. Browse to to the following location: **<Migration Utility Install Folder>\bin**
2. Open the **Migration.sh** file and update the **CHECK\_AC\_SERVICES** value to **false**, as demonstrated in the following before and after sample:

**Before Modification:**

```
CHECK_AC_SERVICES=true
MU_OPTS="--xref href="http://check.ac/">check.ac.services=$CHECK_AC_SERVICES"
```

**After Modification:**

```
CHECK_AC_SERVICES=false
MU_OPTS="--xref href="http://check.ac/">check.ac.services=$CHECK_AC_SERVICES"
```

**NOTE**

If CHECK\_AC\_SERVICES is set to false, then you must also copy the **seos.msg** file. For example: if you have copied DMS\_\_ folder to the /work/backup folder, then you need to copy the seos.msg file **from** either /opt/CA/PAMSCServer/APMS/PAMSC/data **or** /opt/CA/AccessControlServer/APMS/AccessControl/data **to** /work/backup/DMS\_\_ folder.

3. After modifying the migration sh file, re-run the utility.
4. When prompted for the DMS location, provide the backup folder, that is, either **C:\backup\DMS\_\_** or **/work/backup/DMS\_\_**.

**View Server Control Endpoint Agent Status on the Device Agent Status Screen**

Select **Devices**, **Device Agent Status** to access the Device Agent Status screen, which shows the status, version, and other information about PAM SC Endpoint Agents of all types:

- Server Control Agents
- UNAB Agents
- PUPM Agents

The following screen shot shows an example **Device Agent Status** screen, which contains the following two panels:

- **Device Agent Summary**
- **Device Agent Status**

Dashboard
Access
Sessions
Users
Services
Devices
Credentials
Policies
Settings
Configuration

### Device Agent Summary

11 Server Control

1 UNAB

4 PUPM

Uninitialized 4

Active 7

Warning 0

Inactive 0

Active 0

Warning 0

Inactive 1

Active 4

Warning 0

Inactive 0

### Device Agent Status

Column: Value: Filter Reset Add Filter My Views

| Name                             | Address       | Operating System | Server Control Agent Version | UNAB Agent Version   | PUPM Agent Version  |
|----------------------------------|---------------|------------------|------------------------------|----------------------|---------------------|
| cy-2k19141ep                     | 10.131.59.42  | Windows 2016     | ✓ ACW:14.10.20.25            |                      |                     |
| cy-r77sc141cp2 dhcp.broadcom.net | 10.131.58.250 | Linux            | ✓ ACU:14.10.0.1494           |                      | ✓ PUPM:14.10.0.1494 |
| cy-scga141ep                     | 10.131.59.205 | Windows 2016     | ✓ ACW:14.10.20.25            |                      | ✓ PUPM:14.10.20.25  |
| cy-w12r128cp3                    | 10.131.59.49  | Windows 2012     | N/A ACW:12.81.3673           |                      |                     |
| cy-w16128cp3                     | 10.131.58.224 | Windows 2016     | ✓ ACW:12.81.3673             |                      | ✓ PUPM:12.81.3673   |
| cy-wep                           | 10.131.58.105 | Windows 2016     | ✓ ACW:14.10.20.25            |                      |                     |
| lodiibm11ax.pim.com              | 10.131.83.51  | AIX              |                              | ✗ UNAB:12.81.00.3968 |                     |
| lodisun042ao.pim.com             | 10.131.194.43 | Solaris          | ✓ ACU:14.10.0.1546           |                      |                     |
| r77-128cp3ep                     | 10.131.59.219 | Linux            | ✓ ACU:12.81.0.3834           |                      | ✓ PUPM:12.81.0.3834 |
| rhe177-B2                        | 10.131.59.79  | Linux            | N/A ACU:12.81.0.3468         |                      |                     |
| sb039780-ll-ep                   | 10.131.59.229 | Linux            | N/A ACU:14.10.0.1494         |                      |                     |
| tumra02-Win16BN                  | 10.131.59.64  | Windows 2016     | N/A ACW:12.81.3509           |                      |                     |

## Device Agent Summary Section Details

The Device Agent Summary section summarizes counts and status of all Server Control, UNAB, and PUPM agents on endpoint devices.

There are three possible agent statuses, represented by respective boxes:

- **Active:** The agent is active; PAM received the agent heartbeat within the warning status interval.
- **Warning:** PAM has not received the agent heartbeat within the warning status interval.
- **Inactive:** PAM has not received the agent heartbeat within the failure status interval.

### NOTE

The **Uninitialized** box displays agents on devices that are not yet registered or configured with PAM. This state occurs for migrated devices and server control devices that are imported from a CSV file using the Import/Export option.

To filter the agents that are displayed in the **Device Agent Summary** section by type or status, select the corresponding box.

For example, if you select the **Active** box under the **UNAB** box, only UNAB Agents that are in the Active state are listed in the **Device Agent Status** section.

## Device Agent Status Section Details

The Device Agent Status section shows the following status information about agents on endpoint devices:

- **Name:** The hostname of the system on which the agent is installed.
- **Address:** The IP address of the system on which the agent is installed.
- **Operating System:** The operating system of the system on which the agent is installed.
- **Server Control Agent Version:** The status and version of the Server Control Agent, if applicable
- **UNAB Agent Version:** The status and version of the UNAB Agent, if applicable
- **PUPM Agent Version:** The status and version of the PUPM Agent Version, if applicable

Agent status is indicated by the colored icon beside each agent version entry:

- **Green:** The agent is active; PAM received the agent heartbeat within the warning status interval.
- **Yellow:** PAM has not received the agent heartbeat within the warning status interval.
- **Red:** PAM has not received the agent heartbeat within the failure status interval.
- **N/A:** The agent has not been registered with PAM. This state occurs when devices have been migrated from PIM or PAM SC.

Click **Export** to download the status information for all the listed agents (as constrained by any configured filters, if applicable) as a comma-separated value (CSV) file.

### How Agent Status Changes and Agent-Related Actions Are Reflected

The following table shows how agent status changes and agent-related actions are reflected on the **Device Agent Status** screen.

| Agent Status or Agent-related Action                                                                                                                                 | What to expect on the Device Agent Summary screen                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure an access control endpoint.                                                                                                                                | Server Control Agent Status: Active<br>The AC Version, OS, and address details are updated.                                                                                                                  |
| PAM does not receive the next heart beat within the <b>Warning Status Interval</b>                                                                                   | Server Control Agent Status: <b>Warning</b> is updated.                                                                                                                                                      |
| PAM does not receive the next heart beat within the <b>Failure Status Interval</b>                                                                                   | Server Control Agent Status: <b>Inactive</b> is updated.                                                                                                                                                     |
| Migrate an access control endpoint from PIM or PAM SC to PAM.                                                                                                        | Status of Server Control Agent: N/A<br>The Server Control Agent Version, OS, and address are updated.<br>Status and version of PUPM and UNAB are empty.                                                      |
| Delete a <code>pamsc</code> device (in both the UI and in the Device API).                                                                                           | The record related to the device is removed.                                                                                                                                                                 |
| Double-click or select a row in the Agent Status table.                                                                                                              | A dialog opens with the Agent status details.                                                                                                                                                                |
| Configure an access control endpoint to multiple Utility Appliances (UA1 and UA2). Simulate a failover of the UA and check for the details in Agent Status.          | The Agent Status details (Model Window) show the UA info as UA1 as long as UA1 is up and running. When the UA1 goes down and the endpoint is working with UA2, the Agent Status details show UA info as UA2. |
| Change the Utility Appliance configuration from UA1 to UA2, and check for UA info in Agent Status.                                                                   | The UA info shows UA1 initially and then changes to UA2.                                                                                                                                                     |
| Activate the PUPM Agent on an access control endpoint, and configure Utility Appliance in <code>accommon.ini</code> .                                                | The PUPM Agent Status: Active<br>The version, OS, and address are updated. The Utility Appliance Info updates in the Model Window.                                                                           |
| PAM does not receive the next PUPM Agent heartbeat within the <b>Warning Status Interval</b> .                                                                       | PUPM Agent Status updates to <b>Warning</b> .                                                                                                                                                                |
| PAM does not receive the next PUPM Agent heartbeat within the <b>Failure Status Interval</b> .                                                                       | PUPM Agent Status updates to <b>Inactive</b> .                                                                                                                                                               |
| Change the Utility Appliance Configuration from UA1 to UA2 on the endpoint.                                                                                          | The UA info in the model window changes from UA1 to UA2.                                                                                                                                                     |
| Activate a PUPM Agent on the 128 access control endpoint, and configure a Utility Appliance in <code>accommon.ini</code> . Activation requires a TIBCO bridge in UA. | The PUPM Agent Status: Active<br>The version, address, and OS are updated. The Utility Appliance Info is also updated in the Model Window.                                                                   |
| Deploy a Utility Appliance and configure it in PAM.                                                                                                                  | The device details updates in the Agent Status and Model Window.                                                                                                                                             |

## **PAM SC Agent Summary Details**

The following table provides specific information for the different PAM SC Agent types.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Control Agent | <p>The total number of agents includes Active, Warning, Inactive, and Uninitialized (Migrated) agents:</p> <ul style="list-style-type: none"> <li>• SC Agent Active count should match the data in the Agent status details table.</li> <li>• SC Agent Warning count should match the data in the Agent status details table.</li> <li>• SC Agent Inactive count should match the data in the Agent status details table.</li> </ul>                         |
| UNAB Agent           | <p>The total number of agents includes Active, Warning, and Inactive agents:</p> <ul style="list-style-type: none"> <li>• UNAB Agent Active count should match the data in the Agent status details table.</li> <li>• UNAB Agent Warning count should match the data in the Agent status details table.</li> <li>• UNAB Agent Inactive count should match the data in the Agent status details table.</li> </ul>                                             |
| PUPM Agent           | <p>The total number of agents includes Active, Warning, and Inactive agents:</p> <ul style="list-style-type: none"> <li>• PUPM Agent Active count should match the data in the Agent status details table.</li> <li>• PUPM Agent Warning count should match the data in the Agent status details table.</li> <li>• PUPM Agent Inactive count should match the data in the Agent status details table.</li> </ul>                                             |
| Uninitialized        | <ul style="list-style-type: none"> <li>• Count should be equal to the number of migrated and imported devices, but should not include initialized devices.</li> <li>• The Uninitialized section should not be displayed in the summary when the count is 0.</li> <li>• Migrated devices count should match the data in the Agent status details table.</li> <li>• Imported devices count should match the data in the Agent status details table.</li> </ul> |

## **UNAB Agent Summary Details**

The following table provides specific information for UNAB Agents.

|                                                                                      |                                                                                                                     |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| UNAB Agent Status                                                                    | <p>UNAB Agent Status: Active,<br/>The AC Version, OS, and Address details are updated.</p> <p><b>Figure 36:</b></p> |
| PAM does not receive the next heart beat within the <b>Warning Status Interval</b> . | <p>UNAB Agent Status: <b>Warning</b> is updated.</p> <p><b>Figure 37:</b></p>                                       |
| PAM does not receive the next heart beat within the <b>Failure Status Interval</b> . | <p>UNAB Agent Status: <b>Inactive</b> is updated.</p>                                                               |

## **Post Migration Steps**

This content describes procedures that are required after completing migration.

1. Navigate to Access Control Server location:
  - For 12.x.x: /opt/CA/AccessControlServer/APMS/AccessControl/bin/
  - For 14.x.x: /opt/CA/PAMSCServer/APMS/PAMSC/bin/
2. Turn on the access control on the PIM Server and start the PAM SC endpoint services by using the appropriate command:
  - For Windows, enter:
 

```
seosd -start
```
  - For Linux, enter:
 

```
seosd
```
3. Move the PIM Access Control Devices to One PAM:

- Log in to the PIM ENTM.
  - Click on **Policy Management, Policy, Policy, Create Policy**.
  - Enter a Policy Name, such as MigrationPolicy854.
  - Provide the deployment script by clicking the **Policy Script** tab and entering the following:
 

```
So dh-
So dh+ (DH__@<One PAM DS>)
```
  - Click **Submit** to save changes.
4. Click on **Policy Management, Policy, Assignment**.
  5. Check the Agent status summary page:
    - Server Control Agent Status should show Active in the summary.
    - AC Version, OS, and Address details should be updated in the Status table.
    - If PAM does not receive the next heart beat for more than "Warning Status Interval," the Server Control Agent Status shows **Warning** and the count is updated in the summary.
    - If PAM does not receive the next heart beat for more than "Failure Status Interval," the Server Control Agent Status shows **Inactive** and the count is updated in the summary.
  6. Under **Policy Selection**, select the policy that you created when you moved the PIM Access Control Devices to One PAM in an earlier step.
  7. Select the Policy and click **Next**.
  8. Move the Server Control Devices to One PAM:
    - Under **Host Selection**, click **Add** and select the Server Control Devices that you would like to move to One PAM.
    - Select the Hosts and click **Next**.
    - Click on **Finish** to assign the Policy to the hosts.
  9. For testing purposes, restart the policyfetcher on the endpoint. Policyfetcher pulls the policy from the DH and executes it.
  10. Verify both the endpoints are configured against the PAM 4.0 DH by navigating to `selang` and running `so list`.
  11. Restart the policyfetcher on the endpoints so that it sends a heartbeat to PAM.
  12. Log in to PAM and verify that both endpoints are shown in the Device list.
  13. Now that you can manage the endpoints from PAM, deploy a policy on the migrated endpoints. For example:
 

Policy Name: PostMigrationPolicy

Policy Script: eu PostMigrationUser

    - To deploy a policy on demand, **restart** the policyfetcher on the endpoints so that the policy gets deployed faster.
    - Verify the policy that is deployed on the endpoint and the ACL is executed by navigating to `selang` and running `f user`. In this example, you should see the user PostMigrationUser.

## Extract PIM Shared Account Management (SAM) Data

When migrating from PIM to PAM, use the SAM Data Extraction utility to extract Shared Account Management (SAM) data from the Enterprise Manager (ENTM) database. The utility extracts the SAM data (such as Passwords, Endpoints, Accounts, Policies, etc.) into JSON files that you can import into PAM.

The utility supports releases PIM versions 12.8.x, 12.9.x, and 14.x.

### Download the SAM Data Extraction Utility

Download the SAM Data Extraction Utility from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

## **Install the SAM Data Extraction Utility**

### **NOTE**

Install the utility on the ENTM server or any other server that can communicate with the ENTM database.

The software contains two installer files:

- **SAMDataExtraction.bin** for Linux systems
- **SAMDataExtraction.exe** for Windows

### **To install on Linux, follow these steps:**

1. Copy the Utility ISO to the Linux server.
2. Mount the ISO using the following command:  

```
mount -o loop SAMDataExtraction-4.1.0.iso MountLocation
```
3. Navigate to *MountLocation* and locate the installer file named **SAMDataExtraction.bin**.
4. Run the bin file:  

```
./SAMDataExtraction.bin -i console
```
5. Accept the license agreement that appears.
6. Choose the install folder to determine where to install the utility.
7. Choose the database type to determine the type of ENTM database.
8. Provide the database connection details, and then proceed with the installation.

The SAM Data Extraction Utility installation should complete successfully.

### **To install on Windows, follow these steps:**

1. Copy the Utility ISO to the Windows server.
2. Mount the ISO.
3. In the *MountLocation*, locate the **SAMDataExtraction.exe** application and launch it.
4. Follow the prompts and accept the license agreement.
5. Choose the install folder to determine where to install the utility.
6. Choose the database type to determine the type of ENTM database.
7. Provide the database connection details, and then proceed with the installation.

The SAM Data Extraction Utility installation should complete successfully.

## **Run the SAM Data Extraction Utility**

Use the following procedure to run the SAM Extraction utility.

### **Follow these steps:**

1. Navigate to the utility installation location.
2. Navigate to the **bin** folder.
3. Open the **application.properties** file in a text editor and update it, as follows:
  - (Optional) Disable unnecessary modules: All the modules are set to **true** by default. Set the flag to **false** for the modules that you do not want to extract. The default configuration appears as follows:

```
job.enable.account_password=true
job.enable.account_password_history=true
job.enable.endpoint=true
job.enable.fwpasswordpolicy=true
job.enable.ppmpasswordpolicy=true
job.enable.users=true
job.enable.groups=true
```

```
job.enable.admin_roles=true
job.enable.privileged_access_roles=true
job.enable.eventforwarder=true
job.enable.ui_settings=true
job.enable.scheduling_config=true
job.enable.password_consumer=true
job.enable.tasks=true
```

4. Set the token ***decrypt.password*** based on the requirement. The default value is **false**. A **false** value means that the extracted passwords will be in encrypted as they are present in the PIM database.

To see the extracted passwords in plain text, set the ***decrypt.password*** token to **true**; If set to **true**, the utility requires the `FIPSSkey.dat` file to decrypt the passwords to plain text: copy the `FIPSSkey.dat` file from the ENTM server, and then place it in the utility `bin` folder. The `FIPSSkey.dat` file is located here on the ENTM server:

```
Jboss_folder\server\default\deploy\IdentityMinder.ear\config\com\netegrity\config\keys
```

5. Depending on your operating system, go to the `bin` folder and then run either `Extraction.bat` (for Windows) or `Extraction.sh` (for Linux).
6. Once the file execution completes, you can find all the extracted SAM data in the `<utility installation location>\output` folder. The output files are in JSON format.

#### NOTE

When you run the extraction utility for the second time, it archives the existing output files to a folder with a time stamp, and then it creates JSON files in the output folder.

The follow screen capture shows an output sample for your reference.



This PC > Local Disk (C:) > sam437 > output

| Name                   | Date modified     | Type        |
|------------------------|-------------------|-------------|
| 2022-01-11050149       | 1/11/2022 5:01 AM | File folder |
| 2022-01-11050232       | 1/11/2022 5:02 AM | File folder |
| AccountPassword        | 1/11/2022 5:02 AM | JSON File   |
| AccountPasswordHistory | 1/11/2022 5:02 AM | JSON File   |
| AdminRoles             | 1/11/2022 5:02 AM | JSON File   |
| EndPoint               | 1/11/2022 5:02 AM | JSON File   |
| FWPasswordPolicy       | 1/11/2022 5:02 AM | JSON File   |
| Groups                 | 1/11/2022 5:02 AM | JSON File   |
| PasswordConsumers      | 1/11/2022 5:02 AM | JSON File   |
| PPMPasswordPolicy      | 1/11/2022 5:02 AM | JSON File   |
| PrivilegedAccessRoles  | 1/11/2022 5:03 AM | JSON File   |
| RemoteSyslog           | 1/11/2022 5:02 AM | JSON File   |
| SchedulingConfig       | 1/11/2022 5:03 AM | JSON File   |
| UiSettings             | 1/11/2022 5:03 AM | JSON File   |
| Users                  | 1/11/2022 5:18 AM | JSON File   |

### **Encryption Utility**

When first installed, the SAM data extraction utility takes the ENTM database connection information, and then encrypts and stores the credentials in the `application.properties` file. The utility uses these credentials to connect to the database every time the user runs the utility to extract data.

If the database credentials change after the initial installation, the utility fails to make a connection and cannot extract data. If this extraction failure happens, you can encrypt the new password and can update it in the `application.properties` file using this two-part process:

- [Generate the encrypted format of the new database password](#)
- [Update the new database password in the `application.properties` file](#)

### **Generate the Encrypted Format of the New Database Password**

1. Navigate to `SAM_data_extraction_utility_install_location\utility`.
2. Depending on the operating system, locate either `Encryption.bat` (Windows) or `Encryption.sh` (Linux).

3. Run the Encryption file with the new password as an argument to generate the encrypted format of the new password. For example:

```
# ./Encryption.sh Notallowed
----ENVIRONMENT-----
Runtime: AdoptOpenJDK OpenJDK 64-Bit Server VM 11.0.10+9
----ARGUMENTS-----
input: Notallowed
password: supersecretz
algorithm: PBKWithMD5AndDES
----OUTPUT-----
lztZ6F9dq4Nve561o9PZ1IVz0duETrZY
```

The encrypted format of the new database password is **lztZ6F9dq4Nve561o9PZ1IVz0duETrZY**.

### **Update the New Database Password in the application.properties File**

1. Navigate to `SAM_data_extraction_utility_install_location\bin` and locate the `application.properties` file.
2. Update the key **spring.datasource.password** with the new database password (encrypted format generated previously). The password key value should be in the format **ENC(<new password>)**. For example

```
#####
Database Properties
#####
spring.datasource.url=jdbc:sqlserver://10.131.59.203:1433;DatabaseName=pim14latest
spring.datasource.username=pim14latest spring.datasource.password=ENC(lztZ6F9dq4Nve561o9PZ1IVz0duETrZY)
spring.datasource.driverClassName=com.microsoft.sqlserver.jdbc.SQLServerDriver
```

## **Upgrade and Migrate PIM and PAM SC Endpoints**

This section describes how to upgrade and migrate the PIM and PAM SC endpoints.

Use the [table of contents](#) to access the topics in this section.

### **Upgrade a Windows Endpoint**

This article provides information about how to upgrade a Windows Endpoint.

#### **Upgrade Using Graphical User Interface**

Use the Product Explorer to upgrade a Windows endpoint. The Product Explorer uses a graphical interface to upgrade an endpoint and provides interactive feedback. The Product Explorer also lets you select among different architecture installations of the product and install the Runtime SDK.

#### **Follow these steps:**

1. Log in to the Windows system as a user with Windows administrative privileges. That is, as the Windows administrator or a member of the Windows Administrators group.
2. Close any applications that are running on the Windows system.
3. Download the Privileged Access Manager Windows Endpoint from the "Endpoints for PAM 4.0" section on [this page](#) on the Broadcom Support site.
4. Mount the ISO. If autorun is enabled, then the Product Explorer automatically appears. Otherwise, navigate to the mounted drive and double-click the `PRODUCTEXPLORERX86.EXE`.

- From the Product Explorer main menu, expand the **Components** folder, select Privileged Access Manager for Windows (*my\_architecture*), then click **Install**.

**NOTE**

The installation option that matches the architecture of the computer indicates an existing installation of endpoint.

A dialog appears asking if you want to perform an upgrade of the endpoint.

- Click **Yes**.
- The InstallShield wizard starts the installation program.
- When the endpoint upgrade is complete, restart the Windows system.

**Upgrade Silently**

To upgrade an endpoint without interactive feedback, upgrade the product silently using the command line.

**Follow these steps:**

- Log in to the Windows system as a user with Windows administrative privileges. That is, as the Windows administrator or a member of the Windows Administrators group.
- Close any applications that are running on the Windows system.
- Download the Privileged Access Manager Windows Endpoint ISO from the "Endpoints for PAM 4.0" section on [this page](#) on the Broadcom Support site.
- Mount the ISO. If you have autorun enabled, the Privileged Access Manager Product Explorer appears.
- Close the Product Explorer if it appears.
- Open a command line and navigate to the following directory on the optical disc drive:

```
\architecture
```

– *architecture*

Defines the architecture abbreviation for the operating system.

**Values:** x64

- Enter the following command:

```
setup /s /v"/qn COMMAND=<keyword> /L*v <Drive>:\<Log_File>.log
```

**NOTE**

To execute a silent installation, accept the license agreement. The *keyword* that is required to accept the license agreement and silently upgrade the endpoint is found at the bottom of the license agreement available when running the installation program.

**Post-Upgrade Task**

Post-upgrade, ensure that you change the value of the **Distribution\_Server** registry entry to the URL of the ActiveMQ Message Queue server. You can find the **Distribution\_Server** registry entry at HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communication.

**Upgrade an AIX Endpoint**

This article provides information about how to upgrade an AIX endpoint.

## Upgrade Using Native Packages

AIX native packaging is a set of GUI and command-line utilities that let you manage individual software packages. With native packages, manage an endpoint installation with the other software installations that are performed using the AIX `installp`.

### NOTE

Privileged Access Manager supports the AIX native package format (`installp`) only.

Follow these steps to upgrade an endpoint using native packages:

1. [Preliminary Steps](#)
2. [Customize the bff Native Package](#)
3. [Upgrade AIX Native Packages](#)

### Preliminary Steps

Before you upgrade an endpoint, perform the following preliminary steps:

1. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
2. Mount the ISO.
3. Navigate to the `NativePackages` directory in the mounted drive, and copy the following installation files to a temporary directory (`pkg_location`) with read/write permission. Example: `/tmp`. Ensure that the temporary directory does not contain any spaces.
  - `_AIX5_PKG_<Version>.tar.z`
  - `customize_eac_bff`
  - `pre.tar`
  - `parameters.tar`

```
cp /<mounted_location>/NativePackages/_AIX5_PKG_<Version>.tar.Z pkg_location
cp /<mounted_location>/NativePackages/pre.tar pkg_location
cp /<mounted_location>/NativePackages/customize_eac_bff pkg_location
cp /<mounted_location>/NativePackages/parameters.tar pkg_location
```
4. Untar `_AIX5_PKG_<Version>.tar.z`. When you untar, the `CAeAC` file is added to the temporary native package directory.
 

```
cd pkg_location
zcat _AIX5_PKG_<Version>.tar.Z | tar xvf -
```

### Customize the bff Native Package

Customize `customize_eac_bff` to accept the license agreement.

You can also specify custom installation settings when you customize a package. To customize a package, extract the installation parameters file from the package, modify as required, and load it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

### NOTE

Do not modify the package manually. Instead, use the script as described in the following procedure to customize the package.

### Follow these steps:

1. Log in as root.
2. Ensure that you have copied the `customize_eac_bff` script file and the `pre.tar` file to a temporary location on the file system.

### WARNING

The disk space must be at least twice the size of the package to hold temporary repackaging files.

## 3. Display the license agreement:

```
customize_eac_bff -a [-d pkg_location] CAeAC
```

Note the keyword that appears at the end of the license agreement inside a square bracket. Specify this keyword in the next step.

## 4. Customize the package to accept the license agreement:

```
customize_eac_bff -w <keyword> -i <install_location> -d [pkg_location] CAeAC*.bff
```

## 5. (Optional) Set the installation parameters file language:

```
customize_eac_bff -r -l lang [-d pkg_location] CAeAC
```

## 6. (Optional) Change the installation directory:

```
customize_eac_bff -i install_location [-d pkg_location] CAeAC
```

**NOTE**

To set up the package for installation into WPARs (Workload Partitions), change the installation location to an unshared file system using the -i option. By default, /opt and /usr are shared file systems and cannot be used for the WPAR product installations.

## 7. (Optional) Change the default encryption files:

```
customize_eac_bff -s -c certfile -k keyfile [-d pkg_location] CAeAC
```

## 8. Get the installation parameters file:

```
customize_eac_bff -g -f tmp_params [-d pkg_location] CAeAC
```

## 9. (Optional) Edit the installation parameters file to suit your installation requirements.

This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to the post-installation script file you want to run.

## 10. (Optional) Set the installation parameters in the customized package:

```
customize_eac_bff -s -f tmp_params [-d pkg_location] CAeAC
```

You can now use the customized package (CAeAC ) to upgrade an endpoint.

**Command: customize\_eac\_bff**

The `customize_eac_bff` command runs the native package customization script for the `bff` native package files. The script works on any available native packages for AIX. To customize a package, the package must be in a read/write directory on the file system.

**NOTE**

For localized script messages, have `pre.tar` file in the same directory as the script file.

This command has the following format:

```
customize_eac_bff -h [-l lang]
customize_eac_bff -a [-d pkg_location] pkg_name
customize_eac_bff -w keyword [-d pkg_location] pkg_name
customize_eac_bff -r [-d pkg_location] [-l lang] pkg_name
customize_eac_bff -i install_loc [-d pkg_location] pkg_name
customize_eac_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
pkg_name
customize_eac_bff -g [-f tmp_params] [-d pkg_location] pkg_name
customize_eac_bff -t temp_dir [-d pkg_location] [pkg_name]
```

• **pkg\_name**

The name of the package (`bff` file) you want to customize.

• **-a**

Displays the license agreement.

- **-c *certfile***

Defines the full pathname of the root certificate file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-d *pkg\_location***

(Optional) Specifies the directory where the package is placed on the file system. If no directory is specified, the script defaults to `/var/spool/pkg`.

- **-f *tmp\_params***

Specifies the full path and name of the installation parameters file to create or retrieve information from.

**NOTE**

If no file is specified when using the `-g` option, the installation parameters are directed to the standard output (stdout).

- **-g**

Gets the installation parameters file and places in the file that is specified in the `-f` option.

- **-h**

Displays command usage. When used with the `-l` option, displays the language code for supported languages.

- **-i *install\_loc***

Sets the installation directory for the package to `install_loc/PAMSC`

- **-k *keyfile***

Defines the full pathname of the root private key file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-l *lang***

Sets the language of the installation parameters file to *lang*. You can set the language only with the `-r` option.

**NOTE**

For a list of supported language codes, run

`-l`

with the

`-h`

option. By default, the installation parameters file is in English.

- **-r**

Resets the package to use default values as in the original package.

- **-s**

Sets the specified package to use inputs from the customized installation parameters file specified in the `-f` option.

- **-t *tmp\_dir***

Sets the temporary directory for installation operations.

**NOTE**

The default temporary directory is `/tmp`.

- **-w *keyword***

Defines the keyword that specifies that you accept the license agreement. Find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the `-a` option.

## Upgrade AIX Native Packages

To manage endpoint installation with other software installations, use a customized AIX native package for upgrades. The AIX native packages (`bff` files) lets an endpoint upgrade on AIX easily.

**WARNING**

Customize the package to specify that you accept the license agreement using a keyword found inside the license agreement.

**Follow these steps:**

1. Log in as root.
2. Stop Privileged Access Manager services, and the kernel module.  

```
InstallDir/bin/secons -sk
```

```
InstallDir/bin/SEOS_load -u
```
3. (Optional) Check the level (version) of the package that you want to install:  

```
installp -l -d pkg_location
```

  - **pkg\_location**  
 Defines the directory where the CAeAC.<version>.bff package is located.  
 For each package in *pkg\_location*, AIX lists the level of the package.
4. Upgrade the customized package using the following command:  

```
installp -aX -d <pkg_location> CAeAC [pkg_level]
```

  - **pkg\_level**  
 Defines the level number of the package that is recorded earlier.

**WARNING**

If an endpoint is upgraded on WPARs, upgrade the installation in the global environment.

AIX starts installing the CAeAC package from the *pkg\_location* directory. The endpoint is now fully upgraded but not started.

5. (Optional) Upgrade on a specific WPAR *wparname*. (Use -A to install on all system WPARs).
  - From global environment:  

```
syncwpar wpar_name
```
  - From WPAR:  

```
syncroot
```

**Upgrade Using Install\_Base**

Use the Install\_Base script to upgrade an endpoint on AIX interactively or silently.

**Follow these steps:**

1. Log in as *root*.
2. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
3. Mount the ISO, and copy the following files to a temporary location:
  - *install\_base*
  - *\_AIX5\_<Version>.tar.Z*
  - *pre.tar*

**WARNING**

Ensure that the directory, where you mount the endpoint ISO, does not contain any empty spaces.

4. Stop Privileged Access Manager services, and the kernel module.  

```
InstallDir/bin/secons -sk
```

```
InstallDir/bin/SEOS_load -u
```
5. Read the license agreement. To run the *install\_base* script, accept the end-user License Agreement. To get the license file name and location, run *install\_base -h*. Note the keyword that appears at the end of the license agreement inside a square bracket. Specify this keyword in the next step.

6. Run the `install_base` script. The `install_base` script starts and, based on your choices, prompts for the appropriate installation questions.

```
install_base [tar_file] [packages] [options]
```

You can provide the following inputs to the `install_base` command.

- **tar\_file**  
(Optional) Defines the name of the tar file containing the Privileged Access Manager installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of the tar file is optional.
- **packages**  
(Optional) Defines the Privileged Access Manager packages to install. If no packages are specified, the installation script considers the same packages that were installed earlier.

#### NOTE

Install the client package before you install any other package. However, you can specify to install the client package together with any other package.

The packages that can be installed are:

- **-all**  
Installs all packages; client package, server package, API package, and the MFSD package. Also enables STOP (-stop option).
- **-api**  
Installs the API package that includes API libraries and sample programs.
- **-client**  
Installs the client package that has the core Privileged Access Manager functionality required for a standalone computer.
- **-mfstd**  
Installs the MFSD package that includes the mainframe synchronization daemon.

#### NOTE

Install the server package before installing the MFSD package.

- **-server**  
Installs the server package, which includes more binaries and scripts (`selogrcd`, `sepmdd`, `sepmddadm`, `secrepsw`). And these binaries and scripts complement the client package. For example, `sepmdd` sets the computer with a Policy Model.
- **options**  
(Optional) Defines extra installation options.

#### NOTE

Installation options that affect Privileged Access Manager functionality, (for example, -stop) can only be specified when you install the *client* package. Installation options that affect the installation process (for example, -verbose) can be specified with any package.

You can specify the following options:

- **-autocfg [response\_file]**  
Runs the installation in silent mode (not in interactive mode). The installation uses the preferences that are stored in the file to respond to the interactive installation process automatically. If a response file is not specified, or if the response file is missing any options, the installation uses preset defaults.  
To create a response file:
  - Use the `-savecfg` option.
  - Edit an installation parameters file, found inside `parameters.tar`

#### WARNING

If you do not specify a response file, use the `-command` option when using the `-autocfg` option.



Consider the following points in a silent installation:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.  
To install any other package or feature, specify the appropriate option as you would in a normal installation.
- The `install_base` command does not print installation details on the screen during installation.  
To view installation messages on the screen during installation, use the `-verbose` option.
- For security reasons, do not specify the Shared Secret that secures SSL communication between the Report Agent and the Distribution Server in a silent installation. To specify the Shared Secret, configure the Report Agent user (`+reportagent`) after installation.

- **-command keyword**

Defines the command that specifies to accept the license agreement. Find this command at the end of the license agreement (inside square brackets). Use it with the `-autocfg` option. To locate the license agreement file, run `install_base -h`

**NOTE**

The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

- **-d target\_dir**

Defines a custom installation directory. The default installation directory is `/opt/CA/PAMSC`

**WARNING**

You cannot put the Privileged Access Manager database in a mounted network file system (NFS).

- **-dns | -nodns**

Creates a lookaside database with or without DNS hosts. The `-nodns` option specifies that Privileged Access Manager does not perform a `nslookup` on any hosts in the DNS during installation.

- **-fips**

Specifies to activate FIPS-only public key (asymmetric) encryption.

- **-force**

Forces the installation to ignore an active new subscriber update ( `sepmc -n` and `subs <pmdb> newsubs (sub_name)` ) and continue the installation. By default, the installation stops and prompts to finish the subscriber update first.

**NOTE**

If you use this option, the new subscriber update fails.

- **-force\_encrypt**

Forces the installation to accept a non-default encryption key without any warning.

**WARNING**

After the upgrade is complete, the encryption key is set to the default.

**NOTE**

Privileged Access Manager also provides SSL, AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options.

- **-force\_install**

Forces the new installation over the already installed version. Use this option to install over the same version.

- **-force\_kernel**

Forces the installation to continue without warning even if an old kernel cannot be unloaded.

**NOTE**

Reboot the computer after the installation is complete.

- **-g groupname**

Defines the name of the group owner of Privileged Access Manager files. The default value is 0.

- **-h | -help**

Displays help.

- **-ignore\_dep**  
Specifies that the installation does *not* check for dependency with other products.
- **-key *encryption\_key***  
Restores the encryption key during an upgrade.

**NOTE**

While you upgrade, use the same encryption key that was used earlier.

- **-lang *lang***  
Defines the language to install an endpoint.
- **-lic\_dir *license\_dir***  
If the license program is not already installed, this parameter defines the license program installation directory.

**NOTE**

The license program is installed to the specified directory only if \$CASHCOMP variable is not defined in the computer environment (it can be defined in /etc/profile.CA). Otherwise, the license program is installed to \$CASHCOMP. If \$CASHCOMP is not defined and -lic\_dir is specified, the license program is installed to the /opt/CA/SharedComponents directory. CAWIN is installed to the same directory as the license package.

- **-nolink**  
Specifies not to create a link to seos.ini in the /etc directory when the endpoint is installed to the default path (/opt/CA/PAMSC).  
Privileged Access Manager creates a link to seos.ini in the /etc directory when the endpoint is installed to a non-default directory. This lets the endpoint to detect the Installation location. Use this option if you are installing to the default path and you do not want to update /etc due to a security requirement.
- **-nolog**  
Specifies that a log is not kept for the installation process. By default, all transactions that are associated with the installation process are stored to *ACInstallDir*/PAMSC\_install.log (where *ACInstallDir* is the installation directory for Privileged Access Manager).
- **-noprofile**  
Specifies not to load /etc/profile.CA to the user environment.
- **-post *program\_name***  
Specifies a program to run after the installation is complete.
- **-pre *program\_name***  
Specifies a program to run before the installation starts.
- **-rcert *certificate.pem***  
Specifies the full path name to the root certificate file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( def\_root.pem ).

- **-rkey *certificate.key***  
Specifies the full path name to the root key file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( def\_root.pem ).

- **-rootprop**  
Specifies that the *sepass* changes to the root password are sent to the Policy Model. Set this parameter after the installation is complete using the AllowRootProp token of the seos.ini file.
- **-savecfg *<response\_file>***  
Stores the responses provided during the interactive installation for later use by the *-autocfg* option.
- **-stop**

Enables the use of the STOP (Stack Overflow Protection) feature.

- **-system\_resolve**

Specifies to use system functions, which define a bypass for network caching on the system.

**NOTE**

This option cannot be used on IBM AIX platforms.

- **-v**

Displays the version of the Privileged Access Manager package.

- **-verbose**

Specifies that installation messages are displayed on the screen during installation. This parameter is the default in an interactive installation. Specify this option only to see messages when you use the *-autocfg* option.

## Post-Upgrade Steps

Perform the following post-upgrade steps:

1. Restart the endpoint.

2. Start Privileged Access Manager services.

```
seload
```

3. Verify that the `/etc/seos.ini` link is present and points to the valid `seos.ini` file of the new installation.

```
> ls -l /etc/seos.ini
/etc/seos.ini -> /opt/CA/PAMSC/seos.ini
```

4. Check if the binaries are upgraded to the latest version.

```
issec
```

5. Ensure that you configure the value of the **Distribution\_Server** token to the URL of the ActiveMQ Message Queue server. You can find the **Distribution\_Server** token in the **communication** section of the **accommon.ini** configuration file.

## Upgrade a Linux Endpoint

This article provides information about how to upgrade a Linux endpoint.

### Upgrade Using RPM

Upgrade an endpoint to the latest version using Red Hat Package Manager (RPM). RPM is a command-line utility that builds, installs, queries, verifies, updates, and erases individual software packages. RPM is used on Linux platforms such as Fedora, Red Hat Enterprise Linux, and CentOS.

Instead of a regular installation (`install_base`), use RPM as it manages an installation with other RPM software installations as well.

**TIP**

Use the "`pkginfo | grep CAeAC`" command to check the endpoint versions that are currently installed.

Follow these steps to upgrade an endpoint using native packages:

1. [Preliminary Steps](#)
2. [Customize the RPM Package](#)
3. [Upgrade the RPM Package](#)

### Preliminary Steps

Before you upgrade an endpoint, perform the following preliminary steps:

1. Download the Privileged Access Manager Endpoint Components for UNIX ISO.

2. Mount the ISO.
3. Navigate to the `NativePackages`, `RPMPackages`, `LINUX_Platform` directory in the mounted drive, and copy the following installation files to a temporary directory (`pkg_location`) with read/write permission. Example: `/tmp`. Ensure that the temporary directory does not contain any spaces.
  - `CAeAC.<Version>.rpm`
  - `customize_eac_rpm`
  - `pre.tar`

```
cp /<mounted_location>/NativePackages/RPMPackages/Linux_Platform/CAeAC.<Version>.rpm
  pkg_location
cp /<mounted_location>/NativePackages/RPMPackages/Linux_Platform/pre.tar pkg_location
cp /<mounted_location>/NativePackages/RPMPackages/Linux_Platform/customize_eac_rpm
  pkg_location
```

### Customize the RPM Package

Customize `customize_eac_rpm` to accept the license agreement. The `customize_eac_rpm` command runs the Privileged Access Manager RPM package customization script. The script works on Privileged Access Manager RPM packages only. The script is not intended for use with the license program package.

**Note:** Do not modify the package manually. Instead, use the script as described in the following procedure to customize the RPM package.

#### Follow these steps:

1. Log in as root.
2. Ensure that you have copied the `customize_eac_rpm` script file and the `pre.tar` file to a temporary read/write directory on the file system.
3. Display the license agreement:
 

```
customize_eac_rpm -a [-d pkg_location] pkg_filename
```

Note the keyword that appears at the end of the license agreement inside square brackets. Specify this keyword in the next step.
4. Customize the RPM package to specify that you accept the license agreement using a keyword that appears at the end of the license agreement.
 

```
customize_eac_rpm -u /opt/CA -p pkg_location -d . pkg_filename
```
5. (Optional) Set the language of the installation parameters file.
 

```
customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
```
6. (Optional) Change the default encryption files:
 

```
customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename
```
7. (Optional) Get the installation parameters file:
 

```
customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
```
8. (Optional) Edit the installation parameters file to suit your installation requirements.
 

This file lets you set the installation defaults for the package. For example, activate the `POSTEXIT` setting (remove the preceding `#` character) and point it to a post-installation script file you want to run.
9. (Optional) Set the installation parameters in your customized package:
 

```
customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
```

Use the package to upgrade a Linux endpoint with the customized defaults.

### Command: `customize_eac_rpm`

This command has the following format:

```
customize_eac_rpm -h [-l lang]
```

```

customize_eac_rpm -a [-d pkg_location] pkg_filename
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
  pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
customize_eac_rpm -t tmp_dir [-d pkg_location] pkg_filename

```

- ***pkg\_filename***

Defines the file name of the package you want to customize.

**NOTE**

If you do not specify the -d option, define the full path name of the package file.

- **-a**

Displays the license agreement.

- **◆◆-c certfile**

Defines the full path name of the root certificate file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-d *pkg\_location***

(Optional) Specifies the directory where the package is placed on the file system. If no directory is specified, the script assumes that the full path name to the package file is *pkg\_filename*.

- **-f *tmp\_params***

Specifies the full path and name of the installation parameters file to create or retrieve information from.

**NOTE**

If no file is specified when using the -g option, the installation parameters are directed to the standard output (stdout).

- **-g**

Gets the installation parameters file and places in the file that is specified in the -f option.

- **-h**

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

- **-k *keyfile***

Defines the full path name of the root private key file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-l *lang***

Sets the language of the installation parameters file to *lang*. You can set the language only with the -r option.

**NOTE**

For a list of supported language codes, run -l with the -h option. By default, the installation parameters file is in English.

- **-r**

Resets the package to use default values as in the original package.

- **-s**

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

- **-t *tmp\_dir***

Sets the temporary directory for installation operations. The default temporary directory is /tmp.

- **-u**  
Defines the target directory where you install the product.
- **-p**  
Defines the Access Control package.

### **Upgrade the RPM Package**

To manage the product installation with other software installations, install the customized Privileged Access Manager RPM package.

#### **Follow these steps:**

1. Stop Privileged Access Manager services, and the kernel module.

```
InstallDir/bin/secons -sk
InstallDir/bin/SEOS_load -u
```

2. Run the rpm command to upgrade the CAeAC package.

```
rpm -U --oldpackage CAeAC*.rpm
```

The Privileged Access Manager endpoint upgrades.

### **Upgrade Using Install\_Base**

Use the Install\_Base script to upgrade an endpoint on Linux interactively or silently.

#### **Follow these steps:**

1. Log in as *root*.
2. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
3. Mount the ISO, and copy the following files to a temporary location:
  - install\_base
  - \_Linux\_<Version>.tar.Z
  - pre.tar

#### **WARNING**

Ensure that the directory, where you mount the endpoint ISO, does not contain any empty spaces.

4. Stop Privileged Access Manager services, and the kernel module.

```
InstallDir/bin/secons -sk
InstallDir/bin/SEOS_load -u
```

5. Read the license agreement. To run the install\_base script, accept the end-user License Agreement. To get the license file name and location, run install\_base -h. Note the keyword that appears at the end of the license agreement inside a square bracket. Specify this keyword in the next step.
6. Run the install\_base script. The install\_base script starts and, based on your choices, prompts for the appropriate installation questions.

```
install_base [tar_file] [packages] [options]
```

You can provide the following inputs to the install\_base command.

- **tar\_file**  
(Optional) Defines the name of the tar file containing the Privileged Access Manager installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of the tar file is optional.
- **packages**  
(Optional) Defines the Privileged Access Manager packages to install. If no packages are specified, the installation script considers the same packages that were installed earlier.

**NOTE**

Install the client package before you install any other package. However, you can specify to install the client package together with any other package.

The packages that can be installed are:

- **-all**  
Installs all packages; client package, server package, API package, and the MFSD package. Also enables STOP (-stop option).
- **-api**  
Installs the API package that includes API libraries and sample programs.
- **-client**  
Installs the client package that has the core Privileged Access Manager functionality required for a standalone computer.
- **-mfstd**  
Installs the MFSD package that includes the mainframe synchronization daemon.

**NOTE**

Install the server package before installing the MFSD package.

- **-server**  
Installs the server package, which includes more binaries and scripts (`selogrcd`, `sepmdd`, `sepmddadm`, `secrepsw`). And, these binaries and scripts complement the client package. For example, `sepmdd` sets the computer with a Policy Model.
- **options**  
(Optional) Defines extra installation options.

**NOTE**

Installation options that affect Privileged Access Manager functionality, (for example, -stop) can only be specified when you install the *client* package. Installation options that affect the installation process (for example, -verbose) can be specified with any package.

You can specify the following options:

- **-autocfg [response\_file]**  
Runs the installation in silent mode (not in interactive mode). The installation uses the preferences that are stored in the file to respond to the interactive installation process automatically. If a response file is not specified, or if the response file is missing any options, the installation uses preset defaults.  
To create a response file:
  - Use the `-savecfg` option.
  - Edit an installation parameters file, found inside `parameters.tar`

**WARNING**

If you do not specify a response file, use the `-command` option when using the `-autocfg` option.

Consider the following points in a silent installation:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.  
To install any other package or feature, specify the appropriate option as you would in a normal installation.
- The `install_base` command does not print installation details on the screen during installation.  
To view installation messages on the screen during installation, use the `-verbose` option.
- For security reasons, do not specify the Shared Secret that secures SSL communication between the Report Agent and the Distribution Server in a silent installation. To specify the Shared Secret, configure the Report Agent user (`+reportagent`) after installation.
- **-command keyword**

Defines the command that specifies to accept the license agreement. Find this command at the end of the license agreement (inside square brackets). Use it with the `-autocfg` option. To locate the license agreement file, run `install_base -h`

**NOTE**

The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

- **-d *target\_dir***

Defines a custom installation directory. The default installation directory is `/opt/CA/PAMSC`

**WARNING**

You cannot put the Privileged Access Manager database in a mounted network file system (NFS).

- **-dns | -nodns**

Creates a lookaside database with or without DNS hosts. The `-nodns` option specifies that Privileged Access Manager does not perform a `nslookup` on any hosts in the DNS during installation.

- **-fips**

Specifies to activate FIPS-only public key (asymmetric) encryption.

- **-force**

Forces the installation to ignore an active new subscriber update ( `sepmc -n` and `subs <pmdb> newsubs (sub_name)` ) and continue the installation. By default, the installation stops and prompts to finish the subscriber update first.

**NOTE**

If you use this option, the new subscriber update fails.

- **-force\_encrypt**

Forces the installation to accept a non-default encryption key without any warning.

**WARNING**

After the upgrade is complete, the encryption key is set to the default.

**NOTE**

Privileged Access Manager also provides SSL, AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options.

- **-force\_install**

Forces the new installation over the already installed version. Use this option to install over the same version.

- **-force\_kernel**

Forces the installation to continue without warning even if an old kernel cannot be unloaded.

**NOTE**

Reboot the computer after the installation is complete.

- **-g *groupname***

Defines the name of the group owner of Privileged Access Manager files. The default value is 0.

- **-h | -help**

Displays help.

- **-ignore\_dep**

Specifies that the installation does *not* check for dependency with other products.

- **-key *encryption\_key***

Restores the encryption key during an upgrade.

**NOTE**

While you upgrade, use the same encryption key that was used earlier.

- **-lang *lang***

Defines the language to install an endpoint.

- **-lic\_dir *license\_dir***

If the license program is not already installed, this parameter defines the license program installation directory.



**NOTE**

The license program is installed to the specified directory only if \$CASHCOMP variable is not defined in the computer environment (it can be defined in /etc/profile.CA ). Otherwise, the license program is installed to \$CASHCOMP. If \$CASHCOMP is not defined and -lic\_dir is specified, the license program is installed to the /opt/CA/SharedComponents directory. CAWIN is installed to the same directory as the license package.

- **-nolink**

Specifies not to create a link to seos.ini in the /etc directory when the endpoint is installed to the default path (/opt/CA/PAMSC).

Privileged Access Manager creates a link to seos.ini in the /etc directory when the endpoint is installed to a non-default directory. This lets the endpoint to detect the Installation location. Use this option if you are installing to the default path and you do not want to update /etc due to a security requirement.

- **-nolog**

Specifies that a log is not kept for the installation process. By default, all transactions that are associated with the installation process are stored to *ACInstallDir*/PAMSC\_install.log (where *ACInstallDir* is the installation directory for Privileged Access Manager).

- **-noprofile**

Specifies not to load /etc/profile.CA to the user environment.

- **-post program\_name**

Specifies a program to run after the installation is complete.

- **-pre program\_name**

Specifies a program to run before the installation starts.

- **-rcert certificate.pem**

Specifies the full path name to the root certificate file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( def\_root.pem ).

- **-rkey certificate.key**

Specifies the full path name to the root key file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( def\_root.key ).

- **-rootprop**

Specifies that the *sepass* changes to the root password are sent to the Policy Model. Set this parameter after the installation is complete using the *AllowRootProp* token of the seos.ini file.

- **-savecfg <response\_file>**

Stores the responses provided during the interactive installation for later use by the *-autocfg* option.

- **-stop**

Enables the use of the STOP (Stack Overflow Protection) feature.

- **-system\_resolve**

Specifies to use system functions, which define a bypass for network caching on the system.

**NOTE**

This option cannot be used on IBM Linux platforms.

- **-v**

Displays the version of the Privileged Access Manager package.

- **-verbose**

Specifies that installation messages are displayed on the screen during installation. This parameter is the default in an interactive installation. Specify this option only to see messages when you use the *-autocfg* option.

## Post-Upgrade Steps

Perform the following post-upgrade steps:

1. Restart the endpoint.
2. Start Privileged Access Manager services.  

```
seload
```
3. Verify that the `/etc/seos.ini` link is present and points to the valid `seos.ini` file of the new installation.  

```
> ls -l /etc/seos.ini
/etc/seos.ini -> /opt/CA/PAMSC/seos.ini
```
4. Check if the binaries are upgraded to the latest version.  

```
issec
```
5. Ensure that you configure the value of the **Distribution\_Server** token to the URL of the ActiveMQ Message Queue server. You can find the **Distribution\_Server** token in the **communication** section of the **accommon.ini** configuration file.

## Upgrade a Solaris Endpoint

This article provides information about how to upgrade a Solaris endpoint.

### Upgrade Using Native Packages

Upgrade a Solaris endpoint to the latest version using Native Packages. Solaris native packaging provides command-line utilities that create, install, remove, and report on individual software packages.

#### TIP

Tip: Use the `pkginfo|grep CAeAC` command to check the endpoint versions that are currently installed.

Follow these steps to upgrade an endpoint using native packages:

1. [Preliminary Steps](#)
2. [Customize the Solaris Native Package](#)
3. [Upgrade a Solaris Endpoint](#)

### Preliminary Steps

Before you upgrade an endpoint, perform the following preliminary steps:

1. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
2. Mount the ISO.
3. The `NativePackages` directory in the mounted drive contains the Solaris native package for each of the supported Solaris operating systems. Navigate to the `NativePackages` directory in the mounted drive and copy the following installation files to a temporary directory (`pkg_location`) with read/write permission. Example: `/tmp` Ensure that the temporary directory does not contain any spaces.
  - `_Solaris_PKG.<version>.tar.Z`
  - `convert_eac_pkg`
  - `customize_eac_pkg`
  - `pre.tar`
  - `parameters.tar`

```
cp /<mounted_location>/NativePackages/_Solaris_PKG.<version>.tar.Z pkg_location
cp /<mounted_location>/NativePackages/convert_eac_pkg pkg_location
cp /<mounted_location>/NativePackages/customize_eac_pkg pkg_location
```

```
cp /<mounted_location>/NativePackages/parameters.tar pkg_location
cp /<mounted_location>/NativePackages/pre.tar pkg_location
```

4. Untar `_Solaris_PKG_<Version>.tar.z`. When you untar, the `CAeAC` file is added to the temporary native package directory.

```
cd pkg_location
zcat _Solaris_PKG_<Version>.tar.Z | tar xvf -
```

#### **WARNING**

Ensure that file attributes for the entire directory structure of the package are preserved during extraction. Otherwise, the Solaris native packaging tools consider the package corrupt.

5. Verify that your system supports the correct versions of the C++ library.

```
pvs -d /usr/lib/libCstd.so.1
libCstd.so.1;
SUNW_1.1.1;
SUNW_1.1;
SUNW_1.2;
SUNW_1.3;
SUNW_1.3.1;
```

6. Verify that environment variable `LD_LIBRARY_PATH` includes path `/usr/local/lib/`

### **Customize the Solaris Native Package**

Customize `customize_eac_pkg` to accept the license agreement.

You can also specify custom installation settings when you customize a package. To customize a package, extract the installation parameters file from the package, modify as required, and load it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

#### **NOTE**

We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the Privileged Access Manager package.

#### **Follow these steps:**

1. Log in as root.
2. Ensure that you have copied the `customize_eac_pkg` script file and the `pre.tar` file to a temporary location on the file system.
3. Display the license agreement:
 

```
customize_eac_pkg -a -d <pkg_location> CAeAC
```

Note the keyword that appears at the end of the license agreement inside square brackets. Specify this keyword in the next step.
4. Provide the *keyword* to specify that you accept the license agreement:
 

```
customize_eac_pkg -i <install_location> -d . CAeAC
```
5. (Optional) Change the language of the installation parameters file to *lang*. The installation parameters file default language is English.
 

```
customize_eac_pkg -r -l lang -d <pkg_location> CAeAC
```
6. (Optional) Change the default encryption files.
 

```
customize_eac_pkg -s -c certfile -k keyfile -d <pkg_location> CAeAC
```
7. Change the target installation directory from `/tmp` to a custom path. Example: `/opt/CA/`

```
customize_eac_pkg -i /opt/CA -d <pkg_location> CAeAC
```
8. Generate a parameter file with default values.

```
customize_eac_pkg -g -f <pkg_location>/paramtemplate -d <pkg_location> CAeAC
```

9. Modify the default values in the parameter file with data specific to your environment. The parameter file lets you set the installation defaults for the package.

**Example:** You can activate the POSTEXIT setting (by removing the preceding # character) and point it to a post-installation script file you want to run.

### **Command: customize\_eac\_pkg**

The customize\_eac\_pkg command runs the Privileged Access Manager Solaris native package customization script.

- The script works on any of the available product Solaris native packages.
- Move the package to a read/write directory on your file system.
- For localized script messages, have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_eac_pkg -h [-l lang]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
    [pkg_name]
customize_eac_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

- **pkg\_name**  
(Optional) The name of the Privileged Access Manager package you want to customize. If no directory is specified, the script defaults to the main Privileged Access Manager package (CAeAC ).
- **-a**  
Displays the license agreement.
- **-c certfile**  
Defines the full path name of the root certificate file.

#### **NOTE**

This option is applicable to the CAeAC package only.

- **-d pkg\_location**  
(Optional) Specifies the directory where the package is placed on the file system. If no directory is specified, the script defaults to /var/spool/pkg.
- **-f tmp\_params**  
Specifies the full path and name of the installation parameters file to create or retrieve information from.

#### **NOTE**

If no file is specified when using the -g option, the installation parameters are directed to the standard output (stdout).

- **-g**  
Gets the installation parameters file and places it in the file specified by the -f option.
- **-h**  
Displays command usage. When used with the -l option, displays the language code for supported languages.
- **-i install\_loc**  
Sets the installation directory for the package to *install\_loc*/PAMSC.
- **-k keyfile**  
Defines the full path name of the root private key file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-l *lang***

Sets the language of the installation parameters file to *lang*. Set the language only with the -r option.

**NOTE**

For a list of supported language codes, run -l with the -h option. By default, the installation parameters file is in English.

- **-r**  
Resets the package to use default values as in the original package.
- **-s**  
Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.
- **-t *tmp\_dir***  
Sets the temporary directory for installation operations.

**NOTE**

The default temporary directory is /tmp.

- **-w *keyword***  
Defines the keyword that specifies that you accept the license agreement. Find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option. This option is required for new installations and upgrades.

**Upgrade a Solaris Endpoint**

To manage endpoint installation with other software installations, use a customized Solaris native package for upgrades. The native package lets an endpoint upgrade on Solaris easily.

**Follow these steps:**

1. Log in as root.
2. Stop Privileged Access Manager services, and the kernel module.  

```
InstallDir/bin/secons -sk
```

```
InstallDir/bin/SEOS_load -u
```
3. Generate the installation administration file in the <pkg\_location> directory to allow package upgrade.  

```
convert_eac_pkg -p
```

The file myadmin is created from a generic template.
4. Upgrade the Solaris endpoint.  

```
pkgadd -a <pkg_location>/ -d . CAeAC
```

The installer shuts down Privileged Access Manager, and upgrades the endpoint.

**Upgrade Using Install\_Base**

Use the Install\_Base script to upgrade an endpoint on Solaris interactively or silently.

**Follow these steps:**

1. Log in as *root*.
2. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
3. Mount the ISO, and copy the following files to a temporary location:
  - install\_base
  - \_Solaris\_<Version>.tar.Z
  - pre.tar

**WARNING**

Ensure that the directory, where you mount the endpoint ISO, does not contain any empty spaces.

4. Stop Privileged Access Manager services, and the kernel module.

```
InstallDir/bin/secons -sk
```

```
InstallDir/bin/SEOS_load -u
```

5. Read the license agreement. To run the `install_base` script, accept the end-user License Agreement. To get the license file name and location, run `install_base -h`. Note the keyword that appears at the end of the license agreement inside a square bracket. Specify this keyword in the next step.
6. Run the `install_base` script. The `install_base` script starts and, based on your choices, prompts for the appropriate installation questions.

```
install_base [tar_file] [packages] [options]
```

You can provide the following inputs to the `install_base` command.

– **tar\_file**

(Optional) Defines the name of the tar file containing the Privileged Access Manager installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of the tar file is optional.

– **packages**

(Optional) Defines the Privileged Access Manager packages to install. If no packages are specified, the installation script considers the same packages that were installed earlier.

**NOTE**

Install the client package before you install any other package. However, you can specify to install the client package together with any other package.

The packages that can be installed are:

- **-all**  
Installs all packages; client package, server package, API package, and the MFSD package. Also enables STOP (-stop option).
- **-api**  
Installs the API package that includes API libraries and sample programs.
- **-client**  
Installs the client package that has the core Privileged Access Manager functionality required for a standalone computer.
- **-mfstd**  
Installs the MFSD package that includes the mainframe synchronization daemon.

**NOTE**

Install the server package before installing the MFSD package.

- **-server**  
Installs the server package, which includes more binaries and scripts (`selogrcd`, `sepmc`, `sepmdd`, `sepmddadm`, `secrepsw`). And, these binaries and scripts complement the client package. For example, `sepmdd` sets the computer with a Policy Model.
- **options**  
(Optional) Defines extra installation options.

**NOTE**

Installation options that affect Privileged Access Manager functionality can only be specified when you install the *client* package. (Example: -stop) Installation options that affect the installation process can be specified with any package. (Example: -verbose)

You can specify the following options:

- **-autocfg [response\_file]**

Runs the installation in silent mode (not in interactive mode). The installation uses the preferences that are stored in the file to respond to the interactive installation process automatically. If a response file is not specified, or if the response file is missing any options, the installation uses preset defaults.

To create a response file:

- Use the `-savecfg` option.
- Edit an installation parameters file, found inside `parameters.tar`

### WARNING

If you do not specify a response file, use the `-command` option when using the `-autocfg` option.

Consider the following points in a silent installation:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.  
To install any other package or feature, specify the appropriate option as you would in a normal installation.
- The `install_base` command does not print installation details on the screen during installation.  
To view installation messages on the screen during installation, use the `-verbose` option.
- For security reasons, do not specify the Shared Secret that secures SSL communication between the Report Agent and the Distribution Server in a silent installation. To specify the Shared Secret, configure the Report Agent user (`+reportagent`) after installation.
- **-command keyword**  
Defines the command that specifies to accept the license agreement. Find this command at the end of the license agreement (inside square brackets). Use it with the `-autocfg` option. To locate the license agreement file, run `install_base -h`

### NOTE

The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

- **-d target\_dir**  
Defines a custom installation directory. The default installation directory is `/opt/CA/PAMSC`

### WARNING

You cannot put the Privileged Access Manager database in a mounted network file system (NFS).

- **-dns | -nodns**  
Creates a lookaside database with or without DNS hosts. The `-nodns` option specifies that Privileged Access Manager does not perform a `nslookup` on any hosts in the DNS during installation.
- **-fips**  
Specifies to activate FIPS-only public key (asymmetric) encryption.
- **-force**  
Forces the installation to ignore an active new subscriber update ( `sepmc -n` and `subs <pmdb> newsubs (sub_name)` ) and continue the installation. By default, the installation stops and prompts to finish the subscriber update first.

### NOTE

If you use this option, the new subscriber update fails.

- **-force\_encrypt**  
Forces the installation to accept a nondefault encryption key without any warning.

### WARNING

After the upgrade is complete, the encryption key is set to the default.

### NOTE

Privileged Access Manager also provides SSL, AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options.

- **-force\_install**

Forces the new installation over the already installed version. Use this option to install over the same version.

- **-force\_kernel**

Forces the installation to continue without warning even if an old kernel cannot be unloaded.

**NOTE**

Reboot the computer after the installation is complete.

- **-g *groupname***

Defines the name of the group owner of Privileged Access Manager files. The default value is 0.

- **-h | -help**

Displays help.

- **-ignore\_dep**

Specifies that the installation does *not* check for dependency with other products.

- **-key *encryption\_key***

Restores the encryption key during an upgrade.

**NOTE**

While you upgrade, use the same encryption key that was used earlier.

- **-lang *lang***

Defines the language to install an endpoint.

- **-lic\_dir *license\_dir***

If the license program is not already installed, this parameter defines the license program installation directory.

**NOTE**

The license program is installed to the specified directory only if \$CASHCOMP variable is not defined in the computer environment (it can be defined in /etc/profile.CA ). Otherwise, the license program is installed to \$CASHCOMP. If \$CASHCOMP is not defined and -lic\_dir is specified, the license program is installed to the /opt/CA/SharedComponents directory. CAWIN is installed to the same directory as the license package.

- **-nolink**

Specifies not to create a link to seos.ini in the /etc directory when the endpoint is installed to the default path (/opt/CA/PAMSC).

Privileged Access Manager creates a link to seos.ini in the /etc directory when the endpoint is installed to a non-default directory. This lets the endpoint to detect the Installation location. Use this option if you are installing to the default path and you do not want to update /etc due to a security requirement.

- **-nolog**

Specifies that a log is not kept for the installation process. By default, all transactions that are associated with the installation process are stored to *ACInstallDir*/PAMSC\_install.log (where *ACInstallDir* is the installation directory for Privileged Access Manager).

- **-noprofile**

Specifies not to load /etc/profile.CA to the user environment.

- **-post *program\_name***

Specifies a program to run after the installation is complete.

- **-pre *program\_name***

Specifies a program to run before the installation starts.

- **-rcert *certificate.pem***

Specifies the full path name to the root certificate file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( *def\_root.pem* ).

- **-rkey *certificate.key***

Specifies the full path name to the root key file.



**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( `def_root.key` ).

- **-rootprop**  
Specifies that the `sepass` changes to the root password are sent to the Policy Model. Set this parameter after the installation is complete using the `AllowRootProp` token of the `seos.ini` file.
- **-savecfg <response\_file>**  
Stores the responses provided during the interactive installation for later use by the `-autocfg` option.
- **-stop**  
Enables the use of the STOP (Stack Overflow Protection) feature.
- **-system\_resolve**  
Specifies to use system functions, which define a bypass for network caching on the system.

**NOTE**

This option cannot be used on IBM Solaris platforms.

- **-v**  
Displays the version of the Privileged Access Manager package.
- **-verbose**  
Specifies that installation messages are displayed on the screen during installation. This parameter is the default in an interactive installation. Specify this option only to see messages when you use the `-autocfg` option.

**Post-Upgrade Steps**

Perform the following post-upgrade steps:

1. Restart the endpoint.
2. Start Privileged Access Manager services.  
`seload`
3. Verify that the `/etc/seos.ini` link is present and points to the valid `seos.ini` file of the new installation.  
`> ls -l /etc/seos.ini`  
`/etc/seos.ini -> /opt/CA/PAMSC/seos.ini`
4. Check if the binaries are upgraded to the latest version.  
`issec`
5. Ensure that you configure the value of the **Distribution\_Server** token to the URL of the ActiveMQ Message Queue server. You can find the **Distribution\_Server** token in the **communication** section of the **accommon.ini** configuration file.

**Upgrade a Solaris Zones Endpoint**

This article provides information about how to upgrade a Solaris Zones endpoint.

**Upgrade Using Native Packages**

Upgrade on Solaris 10 zones is no different from a regular upgrade. We recommend using Solaris native packaging (`pkgadd` and `pkgrm`) commands to upgrade an endpoint on Solaris 10. When you upgrade the installation in the global zone, the upgrade is propagated into non-global zones automatically.

**WARNING**

For Privileged Access Manager to work in non-global zones, upgrade in the global zone first.

**TIP**

Use the "`pkginfo | grep CAeAC`" command to check the endpoint versions that are currently installed.

Follow these steps to upgrade an endpoint using native packages:

1. [Preliminary Steps](#)
2. [Customize the Solaris Native Packages](#)
3. [Upgrade Solaris Native Package on Solaris Zones](#)
4. [Upgrade on a Solaris Branded Zone](#)
5. [New Zone Setup](#)
6. [Start and Stop CA Privileged Access Manager Server Control in a Zone](#)
7. [Start CA Privileged Access Manager Server Control in a Non-global Zone](#)
8. [Troubleshooting](#)

**Note:** Due to a Solaris 11 limitation, the Privileged Access Manager package is not propagated into non-global zones during installation. We recommend you to install the product in each zone individually using the Solaris native packaging tool (`pkgadd`).

### **Preliminary Steps**

Before you upgrade an endpoint, perform the following preliminary steps:

1. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
2. Mount the ISO.
3. The `NativePackages` directory in the mounted drive contains the Solaris native package for each of the supported Solaris operating systems. Navigate to the `NativePackages` directory in the mounted drive and copy the following installation files to a temporary directory (`pkg_location`) with read/write permission. Example: `/tmp`. Ensure that the temporary directory does not contain any spaces.

- `_Solaris_PKG.<version>.tar.Z`
- `convert_eac_pkg`
- `customize_eac_pkg`
- `pre.tar`
- `parameters.tar`

```
cp /<mounted_location>/NativePackages/_Solaris_PKG.<version>.tar.Z pkg_location
cp /<mounted_location>/NativePackages/convert_eac_pkg pkg_location
cp /<mounted_location>/NativePackages/customize_eac_pkg pkg_location
cp /<mounted_location>/NativePackages/parameters.tar pkg_location
cp /<mounted_location>/NativePackages/pre.tar pkg_location
```

4. Untar `_Solaris_PKG_<Version>.tar.z`. When you untar, the `CAeAC` file is added to the temporary native package directory.

```
cd pkg_location
zcat _Solaris_PKG_<Version>.tar.Z | tar xvf -
```

#### **WARNING**

Ensure that file attributes for the entire directory structure of the package are preserved during extraction, else the Solaris native packaging tools consider the package corrupt.

5. Verify that your system supports the correct versions of the C++ library.

```
pvs -d /usr/lib/libCstd.so.1
libCstd.so.1;
SUNW_1.1.1;
SUNW_1.1;
SUNW_1.2;
SUNW_1.3;
SUNW_1.3.1;
```

6. Verify that environment variable LD\_LIBRARY\_PATH includes path /usr/local/lib/

### **Customize the Solaris Native Packages**

Customize `customize_eac_pkg` to accept the license agreement.

You can also specify custom installation settings when you customize a package. To customize a package, extract the installation parameters file from the package, modify as required, and load it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

#### **NOTE**

We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the Privileged Access Manager package.

#### **Follow these steps:**

1. Log in as root.
2. Display the license agreement:  

```
customize_eac_pkg -a -d <pkg_location> CAeAC
```
3. Note the keyword that appears at the end of the license agreement inside square brackets. Specify this keyword in the next step.
4. Provide the *keyword* to specify that you accept the license agreement:  

```
customize_eac_pkg -w keyword -d <pkg_location> CAeAC
```
5. (Optional) Change the language of the installation parameters file to *lang*. By default, the installation parameters file is in English.  

```
customize_eac_pkg -r -l lang -d <pkg_location> CAeAC
```
6. (Optional) Change the default encryption files.  

```
customize_eac_pkg -s -c certfile -k keyfile -d <pkg_location> CAeAC
```
7. Change the target installation directory from /tmp to a custom path. Example: /opt/CA/:  

```
customize_eac_pkg -i /opt/CA -d <pkg_location> CAeAC
```
8. Generate a response file `paramtemplate` with default values:  

```
customize_eac_pkg -g -f <pkg_location>/paramtemplate -d <pkg_location> CAeAC
```
9. Modify the default values in the `paramtemplate` file with data specific to your environment.  
 The `paramtemplate` file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

#### **NOTE**

Ensure that the parameters for cryptographic options of the DH are the same as those in the environment where `install_base` is installed.

### **Command: customize\_eac\_pkg**

The `customize_eac_pkg` command runs the Privileged Access Manager Solaris native package customization script.

Consider the following points when using this command:

- The script works on any of the available Privileged Access Manager Solaris native packages.
- To customize a package, the package must be in a read/write directory on your file system.
- For localized script messages, have `pre.tar` file in the same directory as the script file.

This command has the following format:

```
customize_eac_pkg -h [-l lang]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
```

```

customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
    [pkg_name]
customize_eac_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]

```

- **pkg\_name**  
(Optional) The name of the Privileged Access Manager package you want to customize. If no directory is specified, the script defaults to the main Privileged Access Manager package (CAeAC ).
- **-a**  
Displays the license agreement.
- **-c certfile**  
Defines the full path name of the root certificate file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-d pkg\_location**  
(Optional) Specifies the directory where the package is placed on the file system. If no directory is specified, the script defaults to /var/spool/pkg.
- **-f tmp\_params**  
Specifies the full path and name of the installation parameters file to create or retrieve information from.

**NOTE**

If no file is specified when using the -g option, the installation parameters are directed to the standard output (stdout).

- **-g**  
Gets the installation parameters file and places it in the file specified by the -f option.
- **-h**  
Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.
- **-i install\_loc**  
Sets the installation directory for the package to *install\_loc*/PAMSC.
- **-k keyfile**  
Defines the full path name of the root private key file.

**NOTE**

This option is applicable to the CAeAC package only.

- **-l lang**  
Sets the language of the installation parameters file to *lang*. Set the language only in conjunction with the -r option.

**NOTE**

For a list of supported language codes run -l with the -h option. By default, the installation parameters file is in English.

- **-r**  
Resets the package to use default values as in the original package.
- **-s**  
Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.
- **-t tmp\_dir**  
Sets the temporary directory for installation operations.

**NOTE**

The default temporary directory is /tmp.

- **-w keyword**

Defines the keyword that specifies that you accept the license agreement. Find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option. This option is required for new installations and upgrades.

**Upgrade Solaris Native Package on Solaris Zones**

To manage endpoint installation with other software installations, use a customized Solaris native package for upgrades. Use the same Privileged Access Manager endpoint version in all zones.

Solaris native packaging may require user interaction by default, and we recommend that configuring the installation as follows to run silently.

**Follow these steps:**

1. Stop Privileged Access Manager services, and the kernel module.

```
InstallDir/bin/secons -sk
InstallDir/bin/SEOS_load -u
```

2. Generate the installation administration file in the <pkg\_location> directory to activate silent installation.

```
convert_eac_pkg -p
```

The file *myadmin* is created from a generic template.

3. Edit the following settings in the *myadmin* file.

```
setuid = nocheck
action = nocheck
```

You have configured the installation administration file to run silently.

4. Install your customized package silently using the -n option.

Do *one* of the following actions:

- To install on all zones, run the following command from the global zone:

```
pkgadd -n -a <pkg_location>\myadmin -d <pkg_location> CAeAC
```

- Install on selected zones:

Run the following command from the global zone:

```
pkgadd -G -n -a <pkg_location>\myadmin -d <pkg_location> CAeAC
```

Run the following command on each of the selected non-global zones:

```
pkgadd -n -a <pkg_location>\myadmin -d <pkg_location> CAeAC
```

Endpoint upgrade is complete.

**Upgrade on a Solaris Branded Zone**

Solaris `pkgadd` does not support propagation of applications that are installed in the Solaris 10 global zone into branded zones. Privileged Access Manager must use `ioctl` instead of a `syscall` to communicate with the kernel module.

**NOTE**

The installation parameter file also lets you install on branded zones automatically when you install on the global zone.

**Follow these steps:**

1. Edit the <pkg\_location>/paramtemplate file, and change the following setting:

```
UseBrandZone = "yes"
```

2. Edit the following line in the *seos.ini* file:

```
SEOS_use_ioctl = 1
```

Privileged Access Manager is configured to use `ioctl`.

3. Install the product in the Solaris 10 branded zone using `pkgadd`.

```
customize_eac_pkg -s -f <pkg_location>/paramtemplate -d <pkg_location> CAeAC
pkgadd -G -a <pkg_location>/myadmin -d <pkg_location> CAeAC
```

4. Install the product in the Solaris 8 and 9 branded zones using `pkgadd`.

```
customize_eac_pkg -s -f <pkg_location>/paramtemplate -d <pkg_location> CAeAC
pkgadd -n -a <pkg_location>/myadmin -d <pkg_location> CAeAC
```

Ignore the warnings and confirm with 'y' when prompted.

The installation is complete. You can now start Privileged Access Manager in the branded zone.

#### **WARNING**

If `SEOS_use_ioctl` is set to 0, modify Privileged Access Manager to use `ioctl` for communication in all zones. Once you make this change and reboot all zones, the installation is complete.

### ***New Zone Setup***

If you install Privileged Access Manager using Solaris native packaging on all zones, Privileged Access Manager automatically installs on any zones you create after the original installation. However, while the post-installation Privileged Access Manager scripts run from within the non-global zone, for new zones, these scripts can only run once the new zone configuration is complete. Specifically, run the "`zlogin -C zonename`" command (which, completes the configuration of the name service, the root password, and so on).

#### **WARNING**

If you do not run the "`zlogin -C zonename`" command, or if you boot and log in to the new zone, Privileged Access Manager installation is incomplete as the post-installation scripts did not run.

### ***Start and Stop CA Privileged Access Manager Server Control in a Zone***

Starting and stopping Privileged Access Manager in Solaris 10 zones is done in the same way you would normally start and stop it on any Solaris computer.

The following exceptions apply to start the product in zones:

- Load the Privileged Access Manager kernel module (`SEOS_load`) from the global zone only.
- Load the Privileged Access Manager kernel module in the global zone before you start Privileged Access Manager in any non-global zone.  
Once the Privileged Access Manager kernel module is loaded in the global zone, you can then start and stop Privileged Access Manager in any non-global zone and in any order.

The following exceptions apply to stopping the product in zones:

- You cannot unload the Privileged Access Manager kernel module when one or more zones has maintenance mode enabled.
- Stop Privileged Access Manager in all zones in any order by issuing the `secons -s` command in each zone.
- Stop Privileged Access Manager in all zones at the same time by adding all zones to a GHOST record and then issuing the `secons -s ghost_name` command from the global zone.  
This is useful, for example, when you want to upgrade Privileged Access Manager across all zones.
- Stop the last zone with the `secons -sk` to disable event interception and prepare the Privileged Access Manager kernel module for unloading.
- You can unload the Privileged Access Manager kernel module (`SEOS_load -u`) from the global zone only.

#### **NOTE**

The `SEOS_load -u` command ensures that Privileged Access Manager is not running on any non-global zone before unloading it.

### ***Start CA Privileged Access Manager Server Control in a Non-global Zone***

You can start the product from any non-global zone just as you would normally, but first load the Privileged Access Manager kernel module in the global zone.

**Follow these steps:**

1. In the global zone, enter the `SEOS_load` command to load the Privileged Access Manager kernel module. The kernel loads and you can now start Privileged Access Manager in any zone.

**NOTE**

The Privileged Access Manager kernel loads but the product does not intercept events in the global zone.

2. In the non-global zone, enter the `seload` command to start the product in that zone. The non-global zone is protected by Privileged Access Manager.

**NOTE**

You can also start Privileged Access Manager in the non-global zone remotely.

**Post-Install Configuration Is Not Complete**

(Solaris only)

**Symptom:**

If Privileged Access Manager is running in the global zone, the installer must unload the kernel before an upgrade. It is possible that the installer fails to unload the kernel, and the switch cannot proceed automatically. You see the following error message:

```
The installer could not unload CA Privileged Access Manager Server Control and switch to the new version.
```

```
The post-install configuration is not complete.
```

```
In order to complete the installation process, choose one of the following options:
```

- Shut down and unload CA Privileged Access Manager Server Control, then run `/opt/CA/PAMSC/sbin/switch_ver.sh`
- Reboot the machine. The installation process continues automatically.

**Solution:**

Follow the instructions in the message to switch manually.

Do *one* of the following:

- Switch manually to the upgraded version without rebooting.
  - a. Shut down Privileged Access Manager.
  - b. Unload Privileged Access Manager.
  - c. Run `/opt/CA/PAMSC/sbin/switch_ver.sh` in the global zone.
  - d. Run `/opt/CA/PAMSC/sbin/switch_ver.sh` in the internal zones.  
The upgraded version of Privileged Access Manager starts running.
- Switch to the upgraded version after rebooting.
  - a. Reboot the machine running the global zone.
  - b. Wait approximately 10 minutes before logging on again.  
The upgraded version of Privileged Access Manager starts running.

**Upgrade Using Install\_Base**

Use the `Install_Base` script to upgrade an endpoint on Solaris interactively or silently.

**Follow these steps:**

1. Log in as *root*.

2. Download the Privileged Access Manager Endpoint Components for UNIX ISO.
3. Mount the ISO, and copy the following files to a temporary location:
  - install\_base
  - \_Solaris\_<Version>.tar.Z
  - pre.tar

**WARNING**

Ensure that the directory, where you mount the endpoint ISO, does not contain any empty spaces.

4. Stop Privileged Access Manager services, and the kernel services.

```
InstallDir/bin/secons -sk
```

```
InstallDir/bin/SEOS_load -u
```

5. Read the license agreement. To run the install\_base script, accept the end-user License Agreement. To get the license file name and location, run install\_base -h. Note the keyword that appears at the end of the license agreement inside a square bracket. Specify this keyword in the next step.
6. Run the install\_base script. The install\_base script starts and, based on your choices, prompts for the appropriate installation questions.

```
install_base [tar_file] [packages] [options]
```

You can provide the following inputs to the install\_base command.

- **tar\_file**  
(Optional) Defines the name of the tar file containing the Privileged Access Manager installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of the tar file is optional.
- **packages**  
(Optional) Defines the Privileged Access Manager packages to install. If no packages are specified, the installation script considers the same packages that were installed earlier.

**NOTE**

Install the client package before you install any other package. However, you can specify to install the client package together with any other package.

The packages that can be installed are:

- **-all**  
Installs all packages; client package, server package, API package, and the MFSD package. Also enables STOP (-stop option).
- **-api**  
Installs the API package that includes API libraries and sample programs.
- **-client**  
Installs the client package that has the core Privileged Access Manager functionality required for a standalone computer.
- **-mfscd**  
Installs the MFSD package that includes the mainframe synchronization daemon.

**NOTE**

Install the server package before installing the MFSD package.

- **-server**  
Installs the server package, which includes more binaries and scripts (selogrcd, sepmd, sepmdm, sepmdadm, secrepsw). And, these binaries and scripts complement the client package. For example, sepmdm sets the computer with a Policy Model.
- **options**  
(Optional) Defines extra installation options.



**NOTE**

Installation options that affect Privileged Access Manager functionality, (for example, `-stop`) can only be specified when you install the *client* package. Installation options that affect the installation process (for example, `-verbose`) can be specified with any package.

You can specify the following options:

- **-autocfg [response\_file]**

Runs the installation in silent mode (not in interactive mode). The installation uses the preferences that are stored in the file to respond to the interactive installation process automatically. If a response file is not specified, or if the response file is missing any options, the installation uses preset defaults.

To create a response file:

- Use the `-savecfg` option.
- Edit an installation parameters file, found inside `parameters.tar`

**WARNING**

If you do not specify a response file, use the `-command` option when using the `-autocfg` option.

Consider the following points in a silent installation:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.  
To install any other package or feature, specify the appropriate option as you would in a normal installation.
- The `install_base` command does not print installation details on the screen during installation.  
To view installation messages on the screen during installation, use the `-verbose` option.
- For security reasons, do not specify the Shared Secret that secures SSL communication between the Report Agent and the Distribution Server in a silent installation. To specify the Shared Secret, configure the Report Agent user (`+reportagent`) after installation.
- **-command keyword**  
Defines the command that specifies to accept the license agreement. Find this command at the end of the license agreement (inside square brackets). Use it with the `-autocfg` option. To locate the license agreement file, run `install_base -h`

**NOTE**

The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

- **-d target\_dir**

Defines a custom installation directory. The default installation directory is `/opt/CA/PAMSC`.

**WARNING**

You cannot put the Privileged Access Manager database in a mounted network file system (NFS).

- **-dns | -nodns**

Creates a lookaside database with or without DNS hosts. The `-nodns` option specifies that Privileged Access Manager does not perform a `nslookup` on any hosts in the DNS during installation.

- **-fips**

Specifies to activate FIPS-only public key (asymmetric) encryption.

- **-force**

Forces the installation to ignore an active new subscriber update ( `sepmc -n` and `subs <pmdb> newsubs (sub_name)` ) and continue the installation. By default, the installation stops and prompts to finish the subscriber update first.

**NOTE**

If you use this option, the new subscriber update fails.

- **-force\_encrypt**

Forces the installation to accept a non-default encryption key without any warning.

**WARNING**

After the upgrade is complete, the encryption key is set to the default.

**NOTE**

Privileged Access Manager also provides SSL, AES (128 bit, 192 bit, and 256 bit), DES, and 3DES encryption options.

- **-force\_install**  
Forces the new installation over the already installed version. Use this option to install over the same version.
- **-force\_kernel**  
Forces the installation to continue without warning even if an old kernel cannot be unloaded.

**NOTE**

Reboot the computer after the installation is complete.

- **-g *groupname***  
Defines the name of the group owner of Privileged Access Manager files. The default value is 0.
- **-h | -help**  
Displays help.
- **-ignore\_dep**  
Specifies that the installation does *not* check for dependency with other products.
- **-key *encryption\_key***  
Restores the encryption key during an upgrade.

**NOTE**

While you upgrade, use the same encryption key that was used earlier.

- **-lang *lang***  
Defines the language to install an endpoint.
- **-lic\_dir *license\_dir***  
If the license program is not already installed, this parameter defines the license program installation directory.

**NOTE**

The license program is installed to the specified directory only if \$CASHCOMP variable is not defined in the computer environment (it can be defined in /etc/profile.CA ). Otherwise, the license program is installed to \$CASHCOMP. If \$CASHCOMP is not defined and -lic\_dir is specified, the license program is installed to the /opt/CA/SharedComponents directory. CAWIN is installed to the same directory as the license package.

- **-nolink**  
Specifies not to create a link to seos.ini in the /etc directory when the endpoint is installed to the default path (/opt/CA/PAMSC).  
Privileged Access Manager creates a link to seos.ini in the /etc directory when the endpoint is installed to a non-default directory. This lets the endpoint to detect the Installation location. Use this option if you are installing to the default path and you do not want to update /etc due to a security requirement.
- **-nolog**  
Specifies that a log is not kept for the installation process. By default, all transactions that are associated with the installation process are stored to *ACInstallDir*/PAMSC\_install.log (where *ACInstallDir* is the installation directory for Privileged Access Manager).
- **-noprofile**  
Specifies not to load /etc/profile.CA to the user environment.
- **-post *program\_name***  
Specifies a program to run after the installation is complete.
- **-pre *program\_name***  
Specifies a program to run before the installation starts.
- **-rcert *certificate.pem***  
Specifies the full path name to the root certificate file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( `def_root.pem` ).

- **-rkey *certificate.key***

Specifies the full path name to the root key file.

**NOTE**

With this option, the script extracts the tar file and then repackages it with the file provided while replacing the default file ( `def_root.key` ).

- **-rootprop**

Specifies that the `sepass` changes to the root password are sent to the Policy Model. Set this parameter after the installation is complete using the `AllowRootProp` token of the `seos.ini` file.

- **-savecfg *<response\_file>***

Stores the responses provided during the interactive installation for later use by the `-autocfg` option.

- **-stop**

Enables the use of the STOP (Stack Overflow Protection) feature.

- **-system\_resolve**

Specifies to use system functions, which define a bypass for network caching on the system.

**NOTE**

This option cannot be used on IBM Solaris platforms.

- **-v**

Displays the version of the Privileged Access Manager package.

- **-verbose**

Specifies that installation messages are displayed on the screen during installation. This parameter is the default in an interactive installation. Specify this option only to see messages when you use the `-autocfg` option.

## Post-Upgrade Steps

Perform the following post-upgrade steps:

1. Restart the endpoint.
2. Start Privileged Access Manager services.  
`seload`
3. Verify that the `/etc/seos.ini` link is present and points to the valid `seos.ini` file of the new installation.  
`> ls -l /etc/seos.ini`  
`/etc/seos.ini -> /opt/CA/PAMSC/seos.ini`
4. Check if the binaries are upgraded to the latest version.  
`issec`
5. Ensure that you configure the value of the **Distribution\_Server** token to the URL of the ActiveMQ Message Queue server. You can find the **Distribution\_Server** token in the **communication** section of the **accommon.ini** configuration file.

## Migrate an Endpoint

Follow the procedure that is described in this article to migrate CA Privileged Identity Manager Endpoint release 12.8 through 14.0, or Privileged Access Manager Endpoint release 14.0 to Privileged Access Manager Endpoint release 14.1.

**Note:** User defined classes and properties are migrated during an endpoint upgrade but not during an endpoint migration.

**Follow these steps:**

**[Source Endpoint]** ♦♦

1. Log in to the source endpoint as a root user (UNIX) or as an administrator (Windows).
2. Stop endpoint services.

[Windows]

```
secons -s
```

[Unix]

```
/opt/CA/PAMSC/bin/secons -sk
```

3. Navigate to the following directory:

[Windows]

```
C:\Program Files\CA\PAMSC\Data\seosdb
```

(UNIX)

```
/opt/CA/PAMSC/seosdb
```

4. Back up the seosdb database:

```
dbmgr -backup backup_directory
```

5. Export the existing rules and the user-related data from the database:

```
dbmgr -export -l -f exported_filename
dbmgr -migrate -r migrated_filename
```

6. Start endpoint services.

[Windows]

```
seosd -start
```

[UNIX]

```
seload
```

**[Destination Endpoint]**

1. Log in to the destination endpoint as a root user (UNIX) or as an administrator (Windows).
2. Stop endpoint services.

[Windows]

```
secons -s
```

[Unix]

```
/opt/CA/PAMSC/bin/secons -sk
```

3. Copy the *exported\_filename* and *migrated\_filename* files from the source endpoint to the destination endpoint to a temporary directory.
4. Modify the *exported\_filename* and *migrated\_filename* files and update the rules that include the PAMSC installation path according to the new installation directory. Example: If the old installation path was C:\Program Files\CA\AccessControl, then the new installation path is C:\Program Files\CA\PAMSC. Please replace all database rules included old path according to the new path.

5. Import into the destination database the existing rules and user-related data that you exported from the source database:

```
selang -l -f exported_filename
dbmgr -migrate -w migrated_filename
```

6. Start endpoint services.

[Windows]

```
seosd -start
```

[UNIX]

```
seload
```

## Associating PAM SC Devices with PAM Devices

If you have duplicate PAM Server Control (SC) devices, you can associate them with a PAM device to reduce device duplication and to make management easier. For example, you might see duplicate PAM SC devices if you are migrating older PIM devices to PAM and PAM was unable to correctly match the PIM device to a PAM SC device.

- You can manually associate a PAM SC device from the Server Control tab. See [Manually Associating a PAM SC Device with a PAM Device](#).
- You can automatically associate multiple PAM SC devices to PAM devices from the Server Control Device Matching tab. See [Automatically Match PAM SC Devices with PAM Devices](#).

Once associated:

- The Agent Status tab and UNAB tab (if the PAM SC device is configured for UNAB) are added to the Manage Devices page. You can edit the device name and address of the PAM SC device on the Manage Devices page.
- All of the groups from the PAM SC device are added to the PAM device, and all of the PAM device group policies (if any) are deployed to the PAM SC device.
- The Server Control tab updates to show the Policies Assigned and Policies Deployed sections.

## Manually Associating a PAM SC Device with a PAM Device

To manually associate a PAM SC device with a PAM device:

1. Log in to the UI.
2. Select **Devices, Manage Devices**.
3. Select the PAM device to associate from the list and then select **Update**.
4. On the Server Control tab, select the search icon and then enter the search criteria for the PAM SC device. The PAM device info appears along with the Server Control Device Name section listing any resulting PAM SC devices.
5. Select the PAM SC device to associate and then select **OK**.

## Changing or Deleting the PAM SC Device Association

To change the PAM SC device that is associated with a PAM device or to remove the association altogether:

1. Log in to the UI.
2. Select **Devices, Manage Devices**.
3. Select the PAM device whose association should be modified from the list and then select **Update**.
4. From the Server Control tab, modify the association:

- To delete the association, select the delete icon next to the Server Control Device Name field. Optionally, delete the PAM SC device name from the Server Control Device Name field and select **OK**.
- To change the association to a different PAM SC device, enter the name of the new device in the Server Control Device Name field and then select **OK**.

If you delete the association between a PAM device and a PAM SC device, PAM performs the following operations:

1. Creates a new PAM device that has a Server Control host but no Device Type set.
2. Associates the PAM SC device with the newly created PAM device.
3. Adds all of the device groups from the existing PAM device to the newly created PAM device. The device groups are not removed from the existing PAM device.

## Automatically Match PAM SC Devices with PAM Devices

You can set PAM to automatically match multiple PAM SC devices with PAM devices. Once configured, PAM searches for matches when you import new SC devices, when SC agents are registered, or when you manually run the duplicate device matching option from the Unmatched Server Control Devices tab. Once matched, you associate them from the Unmatched Server Control Devices tab.

To enable PAM to automatically match multiple PAM SC devices with PAM devices:

1. Log in to the UI.
2. Select **Configuration, Server Control, Device Matching**.
3. On the Duplicate Device Matching Configuration tab, select **Enable Server Control Duplicate Resolution Matching** to configure PAM to search for unassociated PAM SC devices to match with PAM devices.
4. Set how PAM matches PAM SC devices with PAM devices:
  - Set which attribute PAM uses to identify a match. PAM can match the PAM device and PAM SC device by the device names, or by the fully qualified domain name or IP address of the devices. For each attribute you select, also set how strictly PAM compares those attributes.
    - Select **Exact Match** to let PAM match the PAM devices with PAM SC devices that have identical names or IP addresses.
    - Select **Partial Match** to let PAM match PAM devices with PAM SC devices that have similar host names or IP addresses. If you set this option, PAM may match multiple PAM SC devices. You should review the matches and then delete any incorrect matches. See [Deleting Multiple PAM SC Device Associations](#).
    - Select **Disabled** to have PAM ignore this attribute when matching. If you select Disabled, PAM creates a PAM device for each PAM SC device.
  - Select **Enable Automatic Duplicate Device Matching** to have PAM automatically match an SC device if one, and only one, PAM device match is found.
5. When a match is found, it appears in a table on the Unmatched Server Control Devices tab. You can associate a PAM SC device with a PAM device from this tab. See [Associating Device Matches and Running the Device Match Operation](#).

Once associated, the PAM SC device is removed from all customer-visible tables and is managed through the matched PAM device.

To view the status of your PAM SC device matches:

- View which PAM SC devices are matched from the **Matched Server Control Devices** tab of the **Configuration, Server Control Device Matching** page.
- View which PAM SC devices are not matched from the **Unmatched Server Control Devices** tab of the **Configuration, Server Control Device Matching** page. You can also view the status of duplicate device matching operations, and manually run duplicate device matches, from this page.

## Associating Device Matches and Running the Device Match Operation

Matched PAM SC devices appear on the Unmatched Server Control Devices tab of the **Configuration, Server Control** page. From this page you can:

- Review the device matching operation status. This page shows when the device matching operation was last run and what matching criteria was used. This page also shows when the matching criteria were last modified.
- Review the suggested device matches in the Device Match Suggestions table. You can filter the results of this table by column.

Each match includes a patch score. The match score identifies how many times the device matched the attributes that you set when you enabled automatic duplicate device matching. The higher the score, the closer the match.

- Associate the PAM SC devices to the PAM devices by selecting the device matches in the Device Match Suggestions table and then selecting **Match Devices**. Associated PAM SC devices are removed from all customer-visible tables. You manage these devices through the matched PAM device.
- Manually run the device matching operation by selecting **Run Duplicate Device Matching**. You must have enabled PAM to automatically associate multiple PAM SC devices with PAM devices. See [Automatically Match PAM SC Devices with PAM Devices](#).

## Deleting Multiple PAM SC Device Associations

To delete the association between multiple PAM SC devices and their associated PAM devices in one operation:

1. Log in to the UI.
2. Select the **Configuration, Server Control, Matched Server Control Devices** tab.
3. Select the PAM SC devices to disassociate, and click **Unmatch Devices**.

Once the PAM SC devices are disassociated, PAM performs the following operations for each PAM SC device:

1. Creates a new PAM device that has a Server Control host but no Device Type set.
2. Associates the PAM SC device with the newly created PAM device.
3. Adds all of the device groups from the existing PAM device to the newly created PAM device. The device groups are not removed from the existing PAM device.

## Install PAM SC Endpoints

This section describes how to install PAM SC endpoints.

Use the table of contents to access the topics in this section.


### Download the PAM SC Endpoint Installation Software

This procedure describes how to download the 14.1 Endpoint installation software.

Follow these steps:

#### NOTE

Check the 14.1 [Endpoint OS Support Matrix](#) to see if your version of Windows or Linux/Unix is compatible.

1. Open the [Broadcom Support Portal](#) in a new browser session. If you are prompted to log in, use your Broadcom Support credentials.
2. Select **Cyber Security Software** from the product selector (  ) drop-down list that is displayed to the left of your account name in the header.
3. Select **My Downloads** in the left pane.  
The **My Downloads - Cyber Security Software** page opens, listing your licensed products.

4. Select **PRIVILEGED ACCESS MANAGEMENT** from the list.
5. Search for **PAM Server Control MULTI-PLATFORM**.
6. Select **14.1** from the **Release** column, and then select **PAM Server Control MULTI-PLATFORM**.
7. Select the appropriate download:
  - For Windows, select **CA Privileged Access Manager Server Control 14.1 Endpoint Components for Windows DVD500000000001974.iso**.
  - For Linux / Unix, select **CA Privileged Access Manager Server Control 14.1 Endpoint Components for Unix DVD500000000001973.iso**.
8. Use the available controls to download your required component file or files.

**NOTE**

For more information about how to use the controls and generic information about this procedure, select the **Product Download Help** button in the top-right of the screen.

9. If necessary, copy the downloaded file or files to the systems where they are required.

## Install and Uninstall UNIX PAM SC Endpoints Using YUM

This content describes why and how to use YUM to install or uninstall UNIX PAM SC Endpoints. It also shows an example of how to install a PAM SC Endpoint on a UNIX host.

| Problem Statement                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>You want to upgrade from existing PIM/ PAM SC Endpoints to PAM. Your primary requirement is to simplify PAM SC Endpoint installations, upgrades, and patches with <i>no</i> downtime and rollback mechanism in case of failures.</p> <p>Challenges:</p> <ol style="list-style-type: none"> <li>1. Have to copy the builds to thousands of machines.</li> <li>2. Upgrade is time-consuming in case of Large deployments.</li> <li>3. If the upgrade fails, we cannot roll back.</li> </ol> | <p>Simplify PAM SC Endpoint Installation or upgrade using YUM, which creates a central repository (repo) so that the PAM SC Endpoint can pull the software from the repo and install with the following benefits:</p> <ol style="list-style-type: none"> <li>1. Software-Dependency Resolution</li> <li>2. Increased efficiency through automation</li> <li>3. Improved user experience</li> <li>4. Reduce risk if the upgrade fails. You can Roll back to the previous good installation.</li> </ol> |

### Prepare the Repo

Use the following steps to configure a private YUM repo, add the package that contains the rpm to copy to the repo, and then configure.

#### Follow these steps:

1. Configure a private YUM repo on the machine. For example, the repo @ `radra02-I10333` hosts the following rpm packages for testing:
  - CAeAC-1410-0.1141.x86\_64.rpm
  - CAeAC-1401-1.0.616.x86\_64.rpm
  - ca-lic-01.90.04-00.x86\_64.rpm
2. Add the package that contains the rpm to copy to the repo. The following commands add a sample of the package and updates the repo with the new changes:
 

```
radra02-I10333:/var/ftp/pub/PAMRepo/ run
#createrepo --update /var/ftp/pub/PAMRepo/
```
3. Set `pupm_flags` for the account used for auto-login to establish an auto-login session. Otherwise, the session is not established and the session times out. Run the `selang` command shell, and then enter the following `selang` command:



```
editusr <Account that is used for Autologin> pupm_flags(use_original_identity)
```

For example:

```
editusr administrator pupm_flags(use_original_identity)
```

4. Configure the private repo to the Endpoint host by creating the `/etc/yum.repos.d/pam-package.repo` file. The `pam-package.repo` file should include content similar to the following snippet:

```
[pam-package]
name=PAM_PAM SC Endpoint_Repo
baseurl=ftp://radra02-I10333/pub/PAMRepo/
gpgcheck=0
enabled=1
```

5. Run the following command to list `pam-package repo` with packages.

```
#yum repolist
```

The output looks similar to the following snippet:

```
RHEL6_Update_u8
RHEL 6 $releasever Update 8 0
RHEL6_u8 RHEL 6 $releasever Update 8 3,997
pam-package PAM_PAM SC Endpoint_Repo
```

## **Install or Uninstall the Endpoint Using YUM**

Once the private YUM repo is ready, you can install or uninstall the Endpoint using YUM:

- To install the Endpoint, run:  

```
#yum install CAeAC-1410-0.1141.x86_64
```
- To uninstall the Endpoint, run:  

```
#yum erase CAeAC-1410-0.1141.x86_64
```

## **Install a PAM SC Endpoint on a UNIX Host**

This topic describes how to install a PAM SC Endpoint on a UNIX host. Before you proceed with this procedure, you must configure a private YUM repo.

### **Follow these steps:**

1. Run the following command to install the Linux PAM SC Endpoint using YUM:

```
yum install CAeAC-<Version>.<Architecture>.rpm
```

2. Enable the PUPM Agent to enable integration with Privileged Access Manager:

- a. Enter the following command to stop the `seosd` service:

```
/opt/CA/PAMSC/bin/secons -sk
```

- b. Using a standard text editor, open the file `etc/accommon.ini`. Make the following changes:

- Set the tokens in the `accommon.ini` file to the following values:

```
accommon.ini File PupmAgent OperationMode = 1 (default is 0) Communication Distribution Server =
ssl://<hostname>: 61616
```

Where `<hostname>` is the ActiveMQ Broker, such as `pamsc14-integration`

- Enable the PUPM agent as a plugin:

```
Plugins = PupmAgent
```

- Provide the IP of the Distribution Server (Utility Appliance) by replacing the existing `Distribution_Server` IP Address configuration with the actual Utility Appliance IP. For example:

```
Distribution_Server = ssl://10.131.60.166:61616
```

3. Provide the communication password that was specified during the installation of Utility Appliance (the default is "N0tall0wed"):

```
/opt/CA/PAMSC/bin/sechkey -t -pwd "N0tall0wed"
```

4. Load the Access Control daemons:

```
/opt/CA/PAMSC/bin/seload
```

5. Specify the Distribution Server (Utility Appliance) that the PAM SC Endpoint uses for Message Queue communication:

```
/opt/CA/PAMSC/bin/selang
```

```
PAMSC>so dh-
```

```
PAMSC>so dh+ (DH__@Utility Appliance IP)
```

6. Unload the kernel:

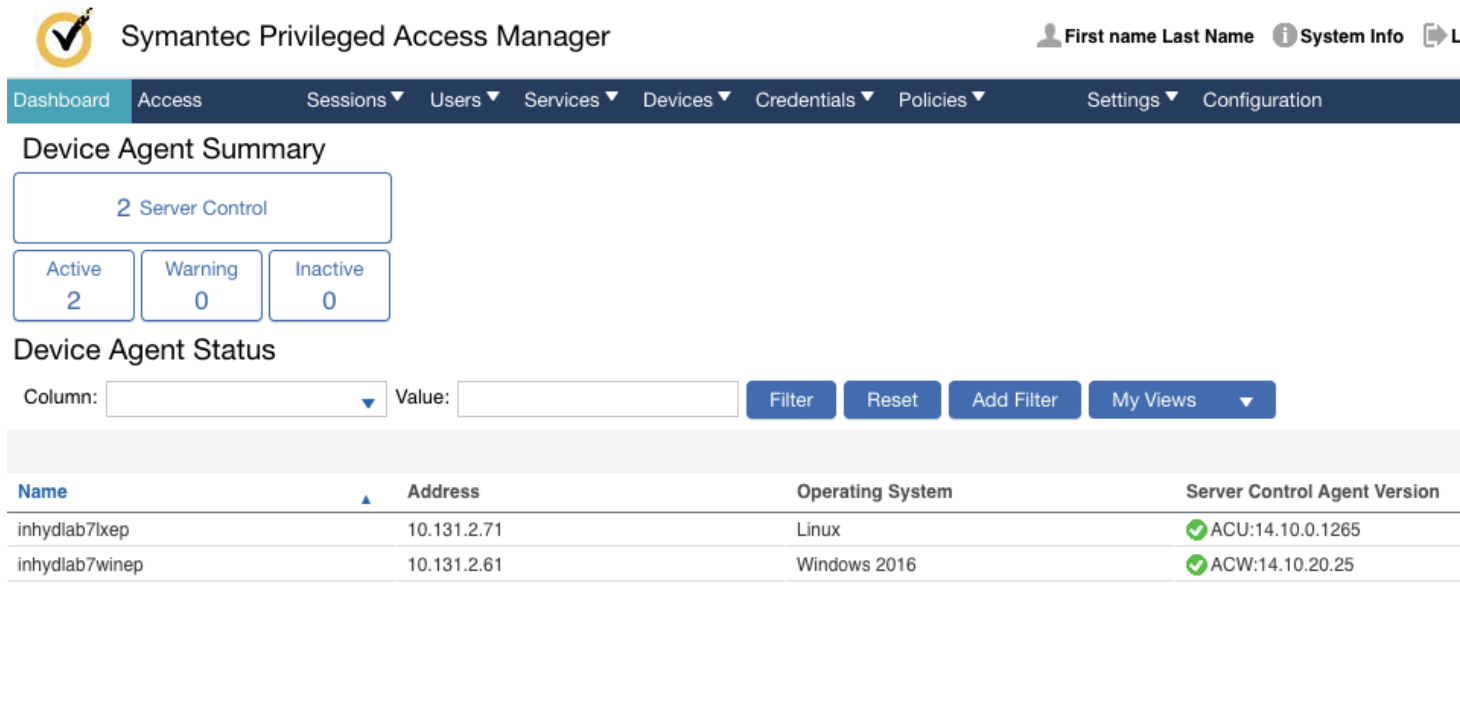
```
/opt/CA/PAMSC/bin/secons -sk
```

7. Reload the Access Control daemons:

```
/opt/CA/PAMSC/bin/seload
```

8. Validate the Server Control Agent is communicating with PAM.

- a. Log into PAM and navigate to Devices/Device Agent Status screen.
- b. Confirm that agent is communicating with PAM.



The screenshot shows the Symantec Privileged Access Manager web interface. The top navigation bar includes links for Dashboard, Access, Sessions, Users, Services, Devices, Credentials, Policies, Settings, and Configuration. The main content area is titled "Device Agent Summary" and shows "2 Server Control" agents. Below this, there are three boxes for "Active" (2), "Warning" (0), and "Inactive" (0). The "Device Agent Status" section includes a filter bar with "Column:" and "Value:" dropdowns, and buttons for "Filter", "Reset", "Add Filter", and "My Views". Below the filter bar is a table with the following data:

| Name           | Address     | Operating System | Server Control Agent Version |
|----------------|-------------|------------------|------------------------------|
| inhydlab7lxep  | 10.131.2.71 | Linux            | ✓ ACU:14.10.0.1265           |
| inhydlab7winep | 10.131.2.61 | Windows 2016     | ✓ ACW:14.10.20.25            |

## Native Package Installation Procedures

If repo is not configured, see the appropriate native package installation information.

### Linux Native Package Installation

- Package filename: CAeAC-<version>.<architecture>.rpm
- Package installation command: rpm -i CAeAC-<version>.<architecture>.rpm

**NOTE**

The installation process uses the source file for the package.

- Package removal command: `rpm -e CAeAC`

**NOTE**

The removal process uses the package name. The source file for the package is not used as the package name.

- Considerations:
  - `rpmbuild` utility must be present to update the package parameters and sign the package.
  - On Linux, you must install the CALic and CAWin packages first.

**Solaris Native Package Installation**

- Package filename: `_SOLARIS_PKG_128.tar.Z`
- Package name: `CAeAC`

**NOTE**

To prevent zone installation problems, install the package from a public directory such as `/var/spool/pkg`.

- Package installation command: `pkgadd [-G] -d <pkg_dir> CAeAC`  
The package is contained in the `CAeAC` directory. Use the `-G` switch to install in a Solaris 10 global zone.
- Package removal command: `pkgrm CAeAC`

**HP-UX Native Package Installation**

- Package filename: `_HPUX11_PKG_128.tar.Z`
- Package name: `CAeAC`
- Package installation command: `swinstall -s <pkg_dir> CAeAC`
- Package removal command: `swremove CAeAC`

**AIX Native Package Installation**

- Package filename: `_AIX_PKG_128.tar.Z`
- Package name: `CAeAC.<version>.bff`
- Package installation command: `installp -ac -d <pkg_dir> CAeAC`
- Package removal command: `removep -u CAeAC`

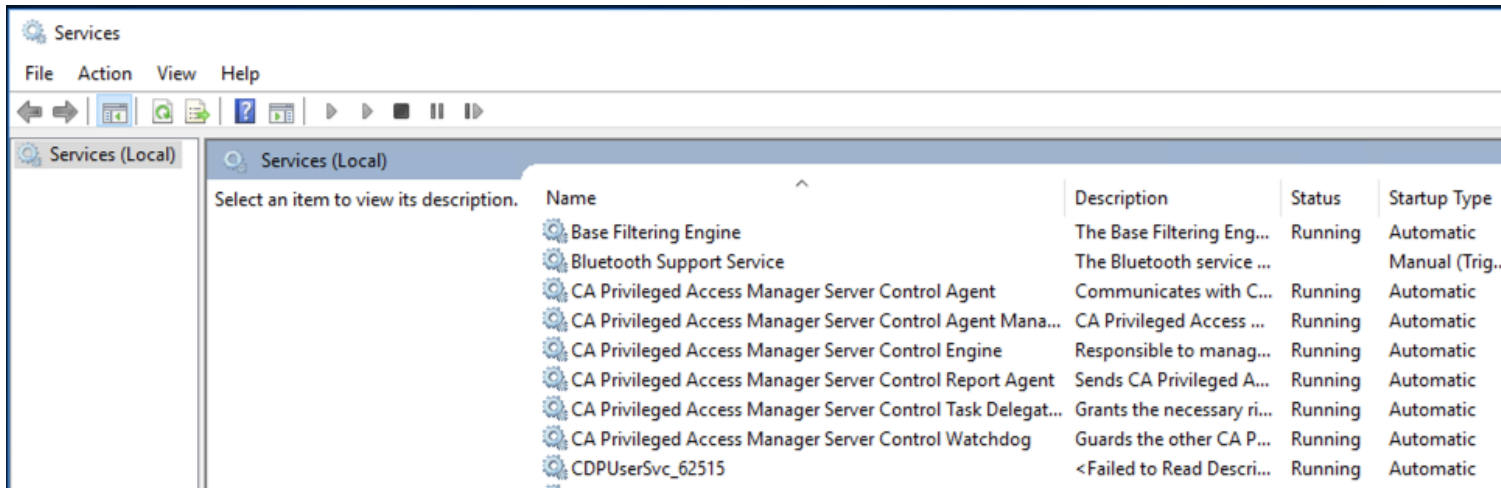
**Install a PAM SC Endpoint on Windows**

You must be a member of the local Administrators group to perform the installation.

The following example describes how to install the endpoint software on Windows using the graphical user interface (GUI):

1. Mount the ISO.
2. Locate the `PRODUCTEXPLORERX86.EXE` executable. Right-click the executable and choose **Run as administrator** to start the installation.
3. From the Components folder of the Product Explorer, select **CA PAMSC for Windows (64-Bit x64)**.
4. Select **Install**.
5. Select the language for the installation and select **OK**.
6. If you are prompted to install the Microsoft Visual C++ Redistributable libraries, select **Install** and wait for the installation to finish.
7. Review the License Agreement, select **I accept the terms of the License Agreement**, and select **Next**.
8. Provide your customer information (user name and organization) and select **Next**. For beta testing, just select **Next**.
9. Select the components to install. Consider the following options:

- If you plan to use PAMSC reporting functionality and audit event collection, select **Report Agent**. Otherwise, leave this item unchecked (the default).
  - Select PUPM Integration to enable integration with Privileged Access Manager, such as login integration.
  - Select the installation directory and select **Next**.
10. Configure the CA PAM SC Administrators and user store:
- Provide DNS domain names to add to the hostname when identifying the endpoint.
  - Provide the names of your PAM SC administrators. You must also identify the servers from which the PAM SC administrators are allowed to manage the endpoint. Typically, this server is the endpoint itself.
- The user installing PAM SC is added as an administrator by default. Do not remove this user or the installation fails. You can remove this user after the installation has completed.
- Select **Next**.
11. Select **Yes** for **Support users and groups from primary stores** (the default) unless there is a specific need to do otherwise. Keeping this setting allows PAM SC to recognize users from the native environment.
- Select **Next**.
12. Configure CA PAM SC communication. Keep the default encryption settings unless the encryption of the server was customized after the installation. The server installation uses AES 256 with the default key and no SSL by default. The client configuration must match the server settings.
- If you want to use SSL:
- Select **Yes** to use Secure Socket Layer (SSL) communication.
  - Leave the **Use Symmetric key encryption** checkbox checked.
- Select **Next**.
13. Select the encryption method to be used for symmetric encryption. 256bit AES is the default and preferred method. Other methods are available for backward capability.
- Typically, the organization specifies a unique encryption key. When symmetric encryption is used, the same key must be used between all endpoints and servers.
14. Enter `DH_@<IP Address Of Utility Appliance (Distribution Server)>` as the Policy Management Server Host. All communication between the endpoint and the PAM Server flows through the Distribution Server (Utility Appliance).
- Select **Next**.
15. Configure audit data collection by specifying when the Report Agent sends audit data to the Event Forwarder. The audit data is used for reporting purposes for SIEM integration.
- Select **Next**.
16. Specify the Distribution Server (Utility Appliance) that the endpoint uses for Message Queue communication. Use the same hostname as specified for Advanced Policy Management screen.
- Also provide the communication key (password) that was specified during the installation of the Utility Appliance (the default is `N0tall0wed`).
- NOTE**  
This setting can also be configured later.
- Select **Next**.
17. Review the installation parameters and select **Next**.
18. Select **Install** and wait for the installation to finish.
19. Select **Finish** to complete the installation.
20. You must reboot the server to load the PAM SC kernel drivers. Select **Yes** to reboot now, or select **No** to manually reboot later.
21. After the server has been rebooted, CA PAM SC components will be automatically started. Validate that all the CA PIM / PAM SC services are running.



22. You need to set `pupm_flags` for the account used for auto login to establish an auto-login session. Otherwise, the session is not established and the session times out. Run the `selang` command shell, and then enter the following `selang` command:

```
editusr <Account that is used for Autologin> pupm_flags(use_original_identity)
```

For example:

```
editusr administrator pupm_flags(use_original_identity)
```

23. Log into the PAM UI and navigate to **Devices, Device Agent Status** screen and confirm that agent is communicating with PAM.

## Uninstall a PAM SC Endpoint from a Windows System

Use one the following methods to uninstall a PAM SC Endpoint from a Windows computer:

### Regular Uninstall

The regular uninstall method uses a graphical interface to uninstall Privileged Access Manager Endpoint and provides interactive feedback.

#### Follow these steps:

1. Log in to the Windows system as a user with Windows administrative privileges. That is, as the Windows administrator or a member of the Windows Administrators group.
  2. (Optional) Stop PAM SC Endpoint services. For more information see, [Start and Stop PAM Server Control Endpoint Services](#)
- Note:** If you do not shut Privileged Access Manager services manually, the installation program shuts.
3. Select **Start, Settings, Control Panel**.  
The Windows Control Panel appears.
  4. Double-click **Add/Remove Programs**.  
The **Add/Remove** dialog appears.
  5. Select Privileged Access Manager Endpoint from the installed programs list and click **Add/Remove**.
  6. Click **Yes** to remove Privileged Access Manager Endpoint.
  7. Click **OK** when the Endpoint uninstallation completes.
  8. Reboot the computer to remove all Privileged Access Manager Endpoint components.

### Silent Uninstall

Use the command line to uninstall Privileged Access Manager Endpoint without interactive feedback.

**Follow these steps:**

1. Log in to the Windows system as a user with Windows administrative privileges. That is, as the Windows administrator or a member of the Windows Administrators group.
2. Enter the following command:

```
Msixexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn insert_params_here
```

The *<insert\_params\_here>* variable specifies the installation settings that you want to pass to the installation program. For example, this command uninstalls Privileged Access Manager and creates an uninstall login c:\ac\_uninst.log:

```
Msixexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:\ac_uninst.log
```

## Install a PAM SC Endpoint on a UNIX Host

This topic describes how to install a PAM SC Endpoint on a UNIX host. Before you proceed with this procedure, you must configure a private YUM repo. For instructions, see [Installing and Uninstalling an Endpoint Using YUM](#).

**Follow these steps:**

1. Run the following command to install the Linux PAM SC Endpoint using yum:

```
yum install CAeAC-<Version>.<Architecture>.rpm
```

2. Enable the PUPM Agent to enable integration with Privileged Access Manager:

- a. Enter the following command to stop the seosd service:

```
/opt/CA/PAMSC/bin/secons -sk
```

- b. Using a standard text editor, open the file etc/accommon.ini. Make the following changes:

- Set the tokens in the acccommon.ini file to the following values:

```
accommon.ini File PupmAgent OperationMode = 1 (default is 0) Communication Distribution Server =  
ssl://<hostname>: 61616
```

Where <hostname> is the ActiveMQ Broker, such as pamscl4-integration

- Enable the PUPM agent as a plugin:

```
Plugins = PupmAgent
```

- Provide the IP of the Distribution Server (Utility Appliance) by replacing the existing Distribution\_Server IP Address configuration with the actual Utility Appliance IP. For example:

```
Distribution_Server = ssl://10.131.60.166:61616
```

3. Provide your PAM SC communication password (default "N0tall0wed"):

```
/opt/CA/PAMSC/bin/sechkey -t -pwd "PAMSC_communication_password"
```

**NOTE**

You can change the default communication password from the **Configuration, Server Control** screen by deselecting the **Use Default** option and specifying a different value.

4. You can change the Load the Access Control daemons:

```
/opt/CA/PAMSC/bin/seload
```

5. Specify the Distribution Server (Utility Appliance) that the PAM SC Endpoint uses for Message Queue communication:

```
/opt/CA/PAMSC/bin/selang
```

```
PAMSC>so dh-
```

```
PAMSC>so dh+ (DH__@Utility Appliance IP)
```

6. Unload the kernel:

```
/opt/CA/PAMSC/bin/secons -sk
```

7. Reload the Access Control daemons:

```
/opt/CA/PAMSC/bin/seload
```

8. Validate that the Server Control Agent is communicating with PAM.
  - a. Log into PAM and navigate to Devices/Device Agent Status screen.
  - b. Confirm that agent is communicating with PAM.

**Symantec Privileged Access Manager**

First name Last Name System Info

Dashboard Access Sessions Users Services Devices Credentials Policies Settings Configuration

### Device Agent Summary

2 Server Control

Active: 2 Warning: 0 Inactive: 0

### Device Agent Status

Column: Value: Filter Reset Add Filter My Views

| Name           | Address     | Operating System | Server Control Agent Version |
|----------------|-------------|------------------|------------------------------|
| inhydlab7lxep  | 10.131.2.71 | Linux            | ✓ ACU:14.10.0.1265           |
| inhydlab7winep | 10.131.2.61 | Windows 2016     | ✓ ACW:14.10.20.25            |

## Native Package Installation Procedures

If repo is not configured, see the appropriate native package installation information.

### Linux Native Package Installation

- Package filename: CAeAC-<version>.<architecture>.rpm
- Package installation command: `rpm -i CAeAC-<version>.<architecture>.rpm`

#### NOTE

The installation process uses the source file for the package.

- Package removal command: `rpm -e CAeAC`

#### NOTE

The removal process uses the package name. The source file for the package is not used as the package name.

- Considerations:
  - The rpmbuild utility must be present to update the package parameters and sign the package.
  - On Linux, you must install the CALic and CAWin packages first.

### Solaris Native Package Installation

- Package filename: `_SOLARIS_PKG_128.tar.Z`
- Package name: CAeAC

#### NOTE

To prevent zone installation problems, install the package from a public directory such as `/var/spool/pkg`.

- Package installation command: `pkgadd [-G] -d <pkg_dir> CAeAC`

The package is contained in the CAeAC directory. Use the -G switch to install in a Solaris 10 global zone.

- Package removal command: `pkgrm CAeAC`

### HP-UX Native Package Installation

- Package filename: `_HPUX11_PKG_128.tar.Z`
- Package name: `CAeAC`
- Package installation command: `swinstall -s <pkg_dir> CAeAC`
- Package removal command: `swremove CAeAC`

### AIX Native Package Installation

- Package filename: `_AIX_PKG_128.tar.Z`
- Package name: `CAeAC.<version>.bff`
- Package installation command: `installp -ac -d <pkg_dir> CAeAC`
- Package removal command: `removep -u CAeAC`

## Use a Warning Period

In addition to deciding what to protect, the implementation team decides how to phase in the new security controls. To minimize disruption to current work patterns, consider an initial period in which you only monitor access to resources, rather than enforcing access restrictions.

You can monitor access by putting the resources into Warning Mode. When Warning Mode is enabled for a resource or a class, and user access violates access restrictions, Privileged Access Manager records a Warning message in the audit log. The product gives the user access to the resource.

**Note:** If you use Warning Mode, consider increasing the maximum size of the audit logs. For more information about Warning Mode, see the *Endpoint Administration* section.

### Privileged Access Manager Backdoor

When you first install Privileged Access Manager, you might incorrectly define rules in the database. Incorrectly defined rules can prevent users from logging in or executing commands. For example, you mistakenly define a rule that denies access to the system directory or to vital parts of the Windows registry.

Because it is difficult to stop the product and fix these mistakes, the product comes with a backdoor that lets you fix these types of problems. Because backdoors can be maliciously exploited, you can disable this backdoor once your system is set up and stable.

To access this backdoor when you start the computer, select the Windows Safe Mode or Safe Mode with Networking from the boot menu. When you select one of these options, the system starts without automatically starting the Privileged Access Manager services.

To disable this backdoor, define the registry value 'LockEE' of the data type `reg_dword` under the registry key `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl\` and set it to 1.

**Note:** This registry value does not exist by default.

Now when you start the system with LockEE set to 1 in:

- Safe Mode, only Privileged Access Manager Engine and Privileged Access Manager Watchdog load. The Privileged Access Manager Agent (and any Policy Models), which rely on network services, do not load.
- Safe Mode with Networking, Privileged Access Manager starts normally.

On UNIX, you can work with Privileged Access Manager in single user mode. When you work in single user mode, the following limitations apply:



- selang is supported in local mode (selang -l) only
- Network classes are not supported
- PMDB functionality (including using selang env pmd) does not work

## Security Implementation Tips

This section provides some implementation information to consider once you have installed Privileged Access Manager.

### **Types of Security**

You can handle security at your site by using one of the following approaches:

- Whatever is not explicitly allowed is forbidden. This is the ideal approach, but it is impossible to use during implementation. Because no rules exist that allow anything to be done on the system, the system blocks all attempts to define access rules. It is like locking yourself out of your car with the keys still in the ignition.
- Whatever is not forbidden is allowed. This approach may be less secure, but it is a practical way to implement a security system.

Privileged Access Manager lets you start with the second approach and, once access rules have been defined, switch to the first approach. Default access (defaccess) and universal access (\_default) rules let you define approach and switch protection policy at any time.

#### **WARNING**

You may need to add all users to the \_restricted group when switching a protection policy. Performance may be significantly affected when switching between protection policies.

### **Accessors**

An *accessor* is an entity that can access resources. The most common type of accessor is a user or group, for whom access authorities should be assigned and checked. When programs access resources, the owner (a user or group) of the program is the accessor. Accessors fall into three categories:

- A person who is associated with a specific user ID
- A person who is a member of a group that has access authority
- A production process that is associated with a certain user ID

The most common type of accessor is a user, a person who can perform a login and for whom access authorities should be assigned and checked. One of the most important features of Privileged Access Manager is accountability. Each action or access attempt is performed on behalf of a user who is held responsible for the request.

Privileged Access Manager lets you define groups of users. Users are usually grouped together by projects, departments, or divisions. By grouping users together, you can significantly reduce the amount of work needed to administer and manage security.

You can define new users and groups and modify existing users and groups through Privileged Access Manager Endpoint Management or through selang commands.

### **Resources**

An essential part of any security policy is deciding which system resources to protect and defining the type of protection these resources receive.

#### ***Resource Classes and Access Rules***

When installed, Privileged Access Manager immediately begins to intercept system events and checks for user authority to access resources. Until you tell the product how to restrict access to your system's resources and which resources to restrict, the result of all authorization checks is to permit access.

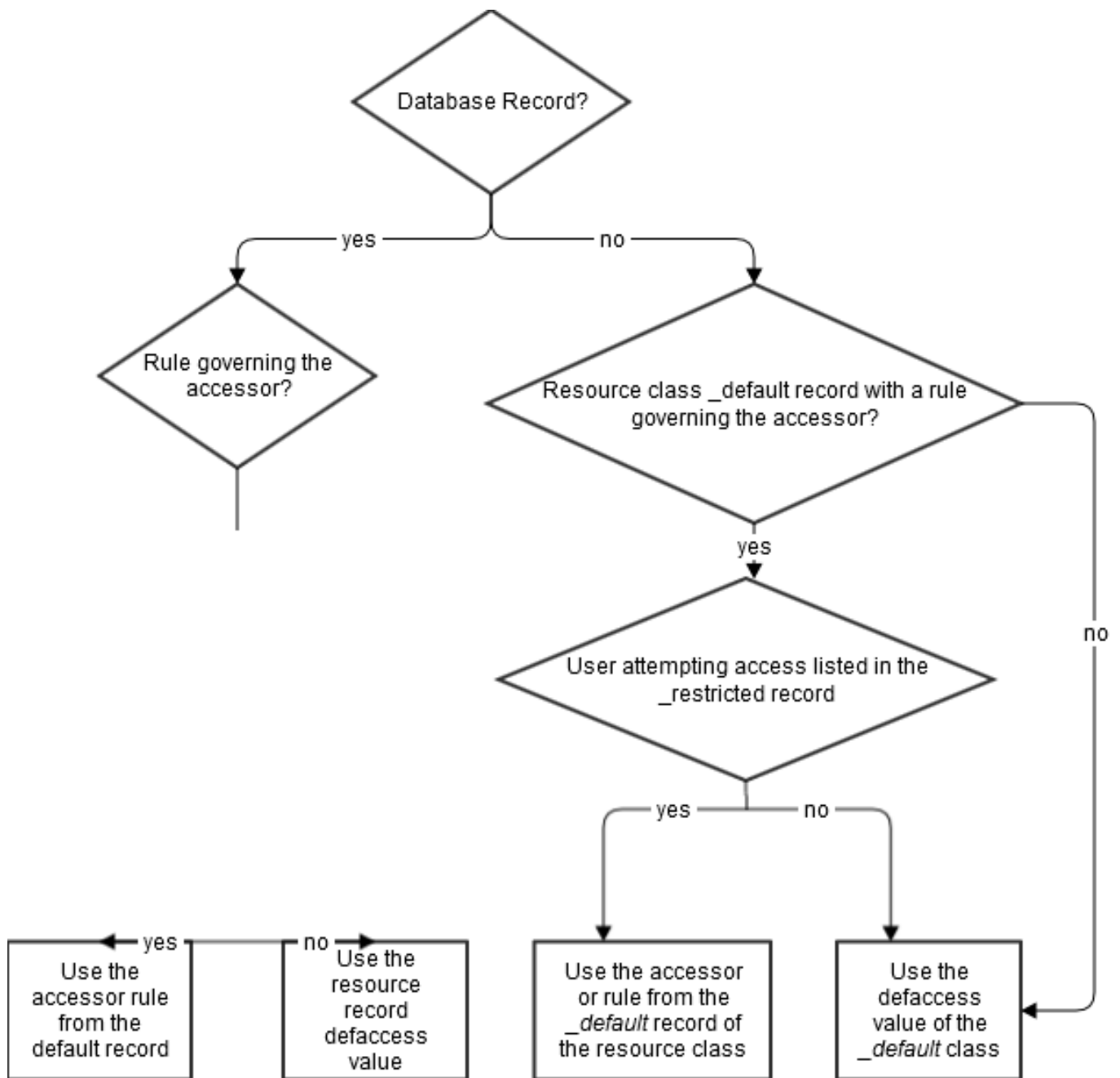
The properties of a protected resource are stored in a resource record. Resource records are grouped into classes. The most important information that is contained in a resource record is the access rules. An *access rule* governs the permission of one or more accessors to work with one or more resources. The following methods are ways to define access rules:

- **Access control list (ACL)**  
A specific list of the accessors authorized to access the resource and the exact access they can have.
- **Negative access control list (NACL)**  
A specific list of the accessors for which access should be denied.
- **Default access for the resource**  
Specifies access rules for accessors that are not listed in an ACL.
- **Universal access** (the `_default` record for a class)  
Specifies access for resources that do not have specific resource records in that class.
- **Program ACL**  
Defines access for a specific accessor through a specific program.
- **Conditional ACL**  
Requires that access depends on some condition. For example, in a TCP record, you can define access to a specific remote host through a specific accessor.
- **Inet ACL**  
Defines access for inbound network activity through specific ports.

### ***Using defaccess and \_default***

When access to a resource is requested, the database is searched in the following order to determine how the request is treated. Privileged Access Manager uses the first access rule that is found. Notice the distinction between *default access* (defaccess) and `_default`.

1. If the resource has a record in the database, and the record has a rule governing the accessor, then Privileged Access Manager uses that rule.
2. If the record exists but does not have a rule governing the accessor, that *record's* default access rule's *defaccess value* is applied to the accessor.
3. If the record does not exist, but in the resource class the `_default` record has a rule governing the accessor, then Privileged Access Manager uses that rule.
4. If the record does not exist, and in the resource class the `_default` record does not have a rule governing the accessor, then the `_default` record's default access rule (the record's defaccess value) is applied to the accessor. For files and registry keys, this applies only to `_restricted` users.

**Figure 38: Resource Class and Access Rules1**

The diagram above shows how the database record is searched to determine which access rules are applied.

**Note:** For more information about resource classes and access rules, see the *selang Reference* section.

## UNAB Endpoint Post Installation Configuration

This content describes how to perform the following two important post-installation configurations procedures:

## Register UNAB Endpoints in Active Directory

To let users defined in the Active Directory log in to UNIX computers, register a UNIX host in the Active Directory server for each UNIX computer on which you installed UNAB.

### Follow these steps on each UNAB Endpoint:

1. Log in to the UNIX/Linux host and become the root user.
2. Register the system with Active Directory by running the following command:

```
/opt/CA/uxauth/bin/uxconsole -register -a <domain user name>
```

For example:

```
root@usliac01aixlab:/opt/CA/uxauth/bin # ./uxconsole -register -a sonvi02 -w 1Qaz2wsx -d gisaclab.local
```

The output is similar to the following:

```
CA Access Control UNAB uxconsole v12.55.0.921 - console utility
Copyright (c) 2010 CA. All rights reserved.

Successfully registered the client.
Starting uxauthd.sh after a 20-second delay to allow for computer object replication in AD ...
UNAB Agent daemon started.
```

Note that registering the system with Active Directory starts the `uxauthd` process.

3. After you have registered the UNIX host in Active Directory, activate UNAB. Activation is the final step in the implementation process of UNAB. Once UNAB is activated, UNAB authenticates users, based on their Active Directory password.

Activate domain authentication by running the following command:

```
root@usliac01aixlab:/ # /opt/CA/uxauth/bin/uxconsole -activate
```

The output is similar to the following:

```
CA Access Control UNAB uxconsole v12.55.0.921 - console utility
Copyright (c) 2010 CA. All rights reserved.

Activation completed successfully.
root@usliac01aixlab:/
```

4. To enable centralized management of UNAB endpoints from the PAM server, configure UNAB for the distribution server (PAM Utility Appliance). This configuration lets users deploy policies to all the UNAB endpoints from a single PAM UI.

- Switch to the `/opt/CA/AccessControlShared/` directory.
- In a standard text editor, modify `accommon.ini` file. Set `Distribution_Server` token to `ssl://<distribution_server:7243>`.

For example, `Distribution_Server = ssl://usilss28-qa.gisaclab.local:7243`

For 12.x (TIBCO), the default TIBCO port is 7243. For PAMSC 14.1 (ACMQ), the default ActiveMQ port is 61616.

- Change directory to `/opt/CA/uxauth/bin`.
- Configure the password for communicating with the Utility Appliance by running the following command:

```
acuxchkey -t -pwd <distribution_server_password>
```

For example:

```
root@usliac01aixlab:/opt/CA/uxauth/bin # ./acuxchkey -t -pwd N0tall0wed
```

The output is similar to the following:

```
CA Access Control UNAB acuxchkey v12.55.0.921
Copyright (c) 2010 CA. All rights reserved.
```

Message queue password updated.

### **Configure UNAB Endpoints to Communicate With a Utility Appliance**

To enable centralized management of UNAB endpoints from the PAM server, UNAB must be configured to communicate with a Utility Appliance. Centralized management of UNAB endpoints allows users to deploy policies to all the UNAB endpoints from the PAM UI.

#### **Follow these steps on each UNAB Endpoint:**

1. Log in to the UNIX or Linux host and become the root user.
2. Change directory to `/opt/CA/AccessControlShared/`.
3. Open the `accommon.ini` file for editing in vi or other preferred text editor.
4. Locate the `Distribution_Server` token and modify its value to reference the IP address and port number of the Utility Appliance: `ssl://<utility_appliance:port>`

For example:

```
Distribution_Server = ssl://usilss28-qa.gisaclab.local:7243
```

5. Configure the password for communicating with the Utility Appliance by running the following command:

```
acuxchkey -t -pwd <utility_appliance_password>
```

For example:

```
/opt/CA/uxauth/bin # ./acuxchkey -t -pwd N0tall0wed
```

## **Server Control Configuration Settings**

Access the **Configuration, Server Control** settings to set endpoint agent status interval, configure a non-default ActiveMQ password, or enable and configure legacy Server Control login integration.

### **Agent Status Interval**

Use the **Agent Status Interval** controls to specify the warning and failure status intervals for Agents (PAM SC Endpoints).

- **Warning Status Interval:** The amount of time expired since the last heartbeat was received by PAM before a warning state is set for the PAM SC Endpoint on a device.
- **Failure Status Interval:** The amount of time expired since the last heartbeat was received by PAM before a failure state is set for the PAM SC Endpoint on a device.

#### **Follow these steps to also see the Agent Status:**

1. To view the status of the device agents, navigate to **Devices, Device Agent Status** to view all agents for Server Control, UNAB, and PUPM devices.
2. Use the Agent Status Interval settings to show agent status, and filter the devices on the Agent Status panel.

See [Agent Status Interval](#) for more information.

### **ActiveMQ Password**

Use the **ActiveMQ Password** option to manage the ActiveMQ password on PAM. By default, when PAM is deployed the password is "N0tall0wed." ActiveMQ sends messages between the PAM server and agents running on endpoints. The ActiveMQ section allows the PAM server to either use the default ActiveMQ password, or enter a new password that is used by all endpoints. This password must match the one used by your endpoints. This password does not override or replace the existing password of an endpoint.

#### **NOTE**

The Server Control Administrator and Configuration manager roles can see (view) the ActiveMQ section; however, these roles cannot change any fields.

To update the ActiveMQ password, the user should be Server Control Administrator, Configuration Manager, and Password Manager. For the Password Manager role, the user must be associated with the ActiveMQ Credential Manager Group. (The Credential Manager Group is installed by default, and comes out-of-the-box.) The superuser, as always, can also change these options.

**To change the ActiveMQ password, follow either one these steps:**

1. Log in to the PAM UI.
2. Select **Configuration, Server Control**.
  - Selecting **Use Default** means that the PAM server uses the default ActiveMQ password, which is N0tall0wed
  - To use a uniform, universal password for all your devices, clear the **Use Default** option, and enter a new password or accept the default in the text fields. The default is "N0tall0wed."

#### NOTE

If you enter a password, the Use Default option becomes unavailable.

### Enable Legacy Server Control Configuration

Set the **Enable Legacy Server Control Configuration** option to configure (or maintain) *legacy* Distribution Servers that were configured in previous PAM versions. PAM continues to support using the legacy integration but without the access control policy management features. This configuration setting is not applicable to new Utility Appliances (which replace Distribution Servers in this release).

#### NOTE

For more information, see [Privileged Access Manager Server Control Login Integration](#).

## Enabling Server Control TLS Settings

Transport Layer Security (**TLS**) is an encryption protocol that protects Internet communications. TLS is an improved version of SSL. The Distribution Host (implemented in the **pam-dh** service) in the Utility Appliance ships with TLS enabled by providing a default root certificate and default public and private keys that were derived from the default root certificate. As a best practice, it is recommended that an administrator replace the default root certificate with your own root certificate (a third-party certificate or a self-signed certificate). As a result of replacing the default root certificate, you need to create new public and private keys derived from the new root certificate.

You, as an administrator, can use the **TLS Settings** screen to specify your own root certificate, a corresponding public key certificate, a corresponding private key, and an optional passphrase for the private key. The contents of the root certificate, public key certificate, and private key with an optional passphrase are represented as Secrets within PAM. The Secrets are referred to in the **TLS Settings** screen by their aliases. The aliases for TLS Settings are collectively referred to as **Distribution Host TLS Aliases**.

After configuring the **TLS Settings**, you can assign them to Utility Groups. OnePAM then distributes the configured root certificate and the public and private keys to individual Utility Groups whenever a Utility Appliance's pam-dh service restarts.

As a last step, modify your UNIX and Windows Endpoints to trust the configured root certificate and enable exclusive TLS communication. For more information, see the [crypto topic](#) that describes the **communication\_mode** parameter for the **[crypto]** section of the **seos.ini** file. Specifically, make sure to set the **communication\_mode** parameter to **ssl\_only** to ensure that data is encrypted. Otherwise, your data may not be using SSL at all.

For more information, see [Enable SSL Encryption](#).

You use this feature by following these general steps:

1. Create Utility Groups containing Utility Appliances, for which you want to apply the TLS settings. See Step 1. Create Utility Groups.
2. Update the Utility Appliances with the proper patches. See Step 2. Updating Utility Appliances.
3. Obtain or create a root certificate. See Step 3. Create or Obtain a Root Certificate.

4. Use your root certificate to produce your server's public and private keys. See Step 4. Generate the Server, Public, and Private Keys.
5. Create a vault, and within the vault, create secrets from the TLS certificates with aliases. Create an authorization for the secrets, mapping the alias for each secret's alias within the vault to a utility group that contains the Utility Appliances to which you want the secrets to apply. See Step 5. Create a Vault and Add Your Secrets.
6. Apply the secrets to the Utility Groups in the **TLS Settings** screen. See Step 6. Enable the TLS Settings.
7. If needed, perform troubleshooting. See Troubleshooting.

### **Step 1. Create Utility Groups**

Before you can apply your TLS settings to your Utility Appliances, you must first create one or more Utility Groups containing one or more Utility Appliances. For more information on creating Utility Groups, see [Add Utility Appliance Devices to Utility Groups](#).

### **Step 2. Updating Utility Appliances**

The TLS settings use two services to help monitor their endpoints and communicate with PAM. Specifically, they appear on the **View Utility Group** window: the **pam-dh** service on the **View Utility Devices** tab, and the **dh-config** service on the **Config Maps** tab.

You need to go to **Configuration**, **Utility**, and then **Patches** to apply any needed patches to every Utility Appliance that uses the TLS settings to make these two services available.

For more information, see [Deploy and Manage Utility Appliance Update Patches](#).

### **Step 3. Create or Obtain a Root Certificate**

You may obtain a third-party X.509 certificate from a certificate authority, or you may create self-signed certificate. One method for creating a self-signed certificate is to use the open-source OpenSSL command-line utility.

### **Step 4. Generate the Server, Public, and Private Keys**

For more information about how to generate the server public and private keys, see [Enable SSL Encryption](#).

Specifically, in the [Use a Server Certificate You Generate from a Third-Party Root Certificate](#) section, see the example in step 5 named **Use seckey to Create a Server Certificate**.

### **Step 5. Create a Vault and Add Your Secrets**

Create a vault or use an existing vault. Within the vault, create secrets with aliases for the root certificate, server public key, and server private key. Optionally, if your public or private key uses a passphrase, you should add that as a secret as well.

Create an authorization for the all of the secrets, mapping the alias for each secret's alias within the vault to a Utility Group that contains the Utility Appliances to which you want the secrets to apply. This action provides authorization so the **pam-dh** service in the Utility Appliance can access the secrets that correspond to each of the aliases when it is restarted.

Note the following items when creating secrets:

- The private key is a binary file; to save the private key as a secret, convert the private key to base64-encoding using a base64 tool.
- You should not schedule any type of future use with TLS secrets. Ensure that when you create a secret, **NONE** of the **Future Use** options are enabled: Specifically, do not enable the **Expire Secret** or **Delete Secret** options.
- Enter only **one** name for the secret's alias in the Aliases field. If you accidentally enter more than one name, PAM only uses the first alias name with TLS settings.
- You cannot update or delete secrets that are currently assigned and are in use as TLS settings.



**Follow these steps:**

1. Make sure that you know the certificates and, optionally, the passphrase you want to add to the vault as secrets.
2. Create a vault or use an existing vault. For more information, see the [Adding or Updating a Vault](#) section in the [Managing Vaults](#) topic.
3. Make the certificates and keys into secrets, and then add your certificates as secrets to that vault. Optionally, if your public or private key uses a passphrase, you must add that as a secret as well. These secrets allow you to distribute your own crypto-certificates using the TLS settings. For more information, see [Adding or Updating a Secret](#).
4. After creating these secrets and their vault, you have to authorize them so they can be accessed. For more information, see [Managing Secret Authorizations \(Mappings\)](#).

**Step 6. Enable the TLS Settings**

As an administrator, you can use the **TLS Settings** screen to enable OnePAM to distribute your own root certificate, as well as the private and private keys to individual Utility Groups. You do this by associating Aliases (collectively known as the **Distribution Host TLS Aliases**) for the root certificate, server public key, and server private key to individual utility groups or to all Utility Groups. Optionally, if your public or private key uses a passphrase, you use that secret's alias as well.

**NOTE**

If you upgrade from 4.0 (or 4.1), all Utility Groups appearing will use the Default TLS alias values.

You cannot use the aliases used with an A2A account. Specifically, when you select **Credentials**, **Manage Targets**, **Accounts**, **Add Account**, and then select A2A as the **Target Account** type with an Alias.

The **TLS Settings** screen has two tabs:

- The **Initial TLS Settings** tab
- The **TLS Settings** tab

**Using the Initial TLS Settings Tab**

The DH component of the Utility Appliance comes with *Default* encryption already configured (expiration in year 2037). This default appears automatically within the **Initial TLS Settings** tab of the **TLS Settings** screen. The default encryption relies on a self-signed certificate, which may not be allowed within some users' production environments.

Use this tab to set the **Distribution Host TLS Aliases**: the root certificate, server public key, server private key, and the private key passphrase alias values to apply to every Utility Group that you create subsequently from saving the values entered here. Specifically, whenever you create a new Utility Group, its alias values populate with the values selected in this tab. You can also choose to immediately and universally apply the values entered in the **Initial TLS Settings** tab to all existing Utility Groups.

**Follow these steps:**

1. Select **Configuration**, **Sever Control**, **TLS Settings**. The **TLS Settings** screen appears, displaying the **Initial TLS Settings** tab. The Utility Appliance's default TLS encryption automatically populates the aliases' fields.
2. Use the **TLS Communication Allowed** option to select the TLS communication version to use with the Utility Group:
  - **All Versions**: This option, the default, enables TLS communication using your current TLS settings setup.
  - **TLS V1.2 Only**: This option enables TLS communications using only TLS V1.2.
3. Use the search icon to filter and select an alias value for the root certificate, server public key, server private key, and the private key passphrase.

**NOTE**

If you select a public key and private key, you must also provide a root certificate alias value. Otherwise, you can leave all fields blank. If you provide a value for either the root certificate, the public key, OR the private key, then you must provide values for all three fields.

4. Select **Save** to apply these values to every Utility Group that you subsequently create from saving the values entered here.



5. Select **Save All and Apply to All Utility Groups** to immediately and universally apply the values entered here to all existing utility groups.

### Using the TLS Settings Tab

Use this tab to set the alias values for the TLS communication version, the root certificate, server public key, server private key, and the private key passphrase for Utility Groups. You can simultaneously select any number of Utility Groups.

You can also display the **View Utility Status** window for a Utility Group by selecting a Utility Group and then selecting the **Status** button. For more information on this window, see [View Utility Group Status](#). This window is also useful for [Troubleshooting](#).

### **Follow these steps:**

1. Select **Configuration, Sever Control, TLS Settings**.
2. Select the **TLS Settings** tab. A list of existing Utility Groups appears. The **Distribution Host TLS Aliases** section lists the current alias values for the TLS communication version, root certificate, server public key, server private key, and the private key passphrase.
3. Select a Utility Group whose **Distribution Host TLS Aliases** you want to edit, and then select **Update**. The **Update <selected utility group name>** window appears, listing the **Distribution Host TLS Aliases**.

#### **NOTE**

You can simultaneously update multiple Utility Groups if you select multiple groups, and then select **Update**. All edits apply to all selected Utility Groups.

4. Choose the TLS communication allowed, or use the search icon to filter and select an alias value for the root certificate, server public key, server private key, and the private key passphrase.

#### **NOTE**

If you select a public key and private key, you must also provide a root certificate alias value. You can otherwise leave any field blank, and PAM uses the default value. If you provide a value for either the root certificate, the public key, OR the private key, then you must provide values for all three fields.

5. Select **OK** to confirm and exit this window. The values entered in this window apply and update the values of the **Distribution Host TLS Aliases** section of the **TLS Settings** tab.

### Troubleshooting

#### Check the Log Files

Select the **View Utility Devices** tab, and then select Log file for pam-dh. If the log displays values for `DH_ROOT`, `DH_PRIVATE`, and `DH_PUBLIC`, a line appears that says:

```
Custom Crypto required = true
```

If there is a value in the log for `DH_PRIVATE_PASSPHRASE`, then a line appears that says:

```
Passphrase required = true
```

The log file also displays any possible errors.

#### Using the Status Button

1. On **TLS Setting** tab, select a Utility Group, and then the **Status** button to display the **View Utility Group** window.
2. Select the **Config Maps** tab. The **Config Map** tab displays the values of Config Map objects (key-value pairs) that determine the behavior of the Utility Appliances in the Utility Group. The **dh-config** section displays the root certificate alias, as well as the public key alias, private key alias, and optional passphrase alias for every Utility Group.

For more information, see [View Utility Group Status](#).

#### Confirming Communication Between OnePAM and an Endpoint

Use these methods to help determine if there is a communication between OnePAM and an endpoint.

- Use the **Deployment Audit** tab on the **Policies, Manage Server Control** screen to view whether your policies have been properly deployed. For more information, see [View Server Control Policy Deployment Audit Data](#). If policies are not deploying properly, there may be an issue with the TLS settings.
- Select **Devices, Device Agent Status** to access the **Device Agent Status** screen, which shows the status, version, and other information about PAM SC Endpoint Agents of all types. For more information, see [View Server Control Endpoint Agent Status on the Device Agent Status Screen](#).
- Examine the **[policyfetcher]** section of the seos.ini file on the endpoint. This file contains various setup and initialization tokens that are used by Privileged Access Manager. For more information, see [policyfetcher](#).

## High Availability

The Enterprise Management Server uses mirrored sites to provide high-availability deployments. *Mirrored* sites are fully redundant facilities with full, real-time information mirroring and are identical to the primary site in all technical aspects. Data is processed and stored at the primary and mirrored sites simultaneously.

Mirrored sites employ an active-passive deployment for failover. An *active-passive* deployment includes two or more data centers, with one actively processing requests and the other ready to service requests if the active one fails. The clustering solution software that you select is responsible for controlling the active and passive servers and switching between them in case of failure.

In an active-passive deployment, the active server is referred to as the primary server, and the passive server is referred to as the secondary server.

## Configure Endpoints for High Availability

After you installed and configured the primary and secondary Enterprise Management Servers, you set up the Privileged Access Manager endpoints to work in a High Availability environment.

### Follow these steps:

1. Install Privileged Access Manager with the Advanced Policy Management Client feature that is enabled on the endpoint.
2. Open a Command Prompt window on the endpoint and enter the following command:

```
dmsmgr -config -dhname names
```

This command configures the endpoint to work with the comma-separated list of Distribution Hosts.

**Note:** For more information about the dmsmgr utility, see the *Reference section*.

3. Set the *Distribution\_Server* configuration setting to list the Distribution Servers, which are separated by a comma:

```
ssl://ds1.sample.com:7243, ssl://ds2.sample.com:7243
```

4. Save the settings.  
You have configured a list of Distribution Hosts and Distribution Servers with which the endpoint can communicate. The endpoint can now work in a High Availability environment.

### Example: Configure a List of Distribution Servers

The following example shows you how to configure a list of Distribution Servers for High Availability.

During the installation of the endpoint, you are asked to enter the parameters of the Distribution Server that the endpoint communicates with. By default, this is the Enterprise Management Server. For High Availability, you configure the endpoint to use the secondary Distribution Server when the primary Distribution Server fails.

1. Enter the names of the primary and secondary Distribution Servers:

```
dmsmgr -config -dhname DH__@node1.computer.com,DH__@node2.computer.com
```

A message appears confirming the action.

2. Specify the list of primary and secondary Distribution Server URLs.
  - **UNIX:** Modify the Distribution\_Server parameter in the [communication] section of accommon.ini file.
  - **Windows:** Modify the Distribution\_Server value in the Windows Registry. This parameter is found in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication
```

## Communication Encryption

You can use the following methods to encrypt communication between Privileged Access Manager components and to encrypt client/server communication:

- Symmetric encryption
- SSL

### NOTE

When you change the encryption mode on Windows (for example, to FIPS-only mode), restart Privileged Access Manager services if you need to propagate passwords from a password PMDB.

## Uninstall HP-UX Package

To uninstall a UNAB HP-UX package installation, you need to uninstall the UNAB packages in the reverse order of their installation.

To uninstall Privileged Access Manager packages, uninstall the main UNAB package:

```
swremove unab_package_name
```

- *unab\_package\_name*  
Defines the name of the UNAB native package.

## Configure PAM SC to Protect Your Endpoints

This section describes how to protect your endpoints.

**Use the table of contents to access the topics in this section.**

### Server Control Policy Management Operations

This section describes how to do Server Control policy management operations.

**Use the table of contents to access the topics in this section.**

### Manage and Troubleshoot Server Control Policies

Use the controls on the **Policies, Manage Server Control** panel to create, update, and delete Server Control policies and audit and troubleshoot those policies on Server Control devices and device groups.

This topic describes how to use the default **Server Control Policies** tab to create, update, and delete Server Control policies.

### NOTICE

For information about the auditing and troubleshooting tasks available from the other tabs on the **Manage Server Control** panel, see the following topics:

- [Audit your Server Control policy deployments](#) (**Deployment Audit** tab).
- [Troubleshoot policies on Server Control devices](#) (**Device Troubleshooting** tab).
- [Troubleshoot policies on Server Control device groups](#) (**Device Group Troubleshooting** tab).

## Create a Server Control Policy

Do this procedure to create a Server Control Policy.

### Follow these steps:

1. Navigate to **Policies, Manage Server Control**.
2. On the **Server Control Policies** tab, select **Add**. The **Add Policy** dialog appears.
3. On the **General** tab, enter the name and description of the policy.
4. On the **Policy Script** tab, load a deploy policy script and an undeploy script by either importing the policy script or typing the `selang` commands directly in the dialog box. For example:

**Policy Script - Use Case:** Limit the scope of superuser "root."

Define a new FILE resource record with a default access of `none` and owner `nobody`. No user should be able to access this file. If you specify an owner as `nobody`, Access Control denies permission even if the logged in user is "root."

### NOTE

The FILE `/tmp/test1` must be present in the file system.

### Selang Script:

```
newres FILE /tmp/test1 owner(nobody) defaccess(none) audit(all)
```

5. In the **Description** field, enter an appropriate description to provide deployment script-specific information.
6. If you have further edits to make on the policy script, unset the **Finalize** option. When your edits are complete, set the **Finalize** option. You cannot deploy a policy script unless the **Finalize** option is selected. The default is checked.
7. On the **Policy Dependency** tab, move the appropriate dependent policies from the **Available Policies** list to the **Selected Policies** list. Assigning the dependent policies is a prerequisite to assign this newly created policy.
8. Select **OK**. The policy that you have now created is listed on the **Server Control Policies** page.

## Copy a Server Control Policy

Do this procedure to copy a Server Control Policy.

### Follow these steps:

1. Navigate to **Policies, Manage Server Control**.
2. On the **Server Control Policies** tab, select the policy to be copied and select **Copy**.
3. On the **General** tab, enter a new name and appropriate description of the policy.
4. Make the appropriate changes in the **Policy Script** tab and the **Policy Dependency** tab.
5. Select **OK**.

The new policy is created and listed on the **Server Control Policies** page.

## Update a Server Control Policy

Do this procedure to update a Server Control Policy.

**Follow these steps:**

1. Navigate to **Policies, Manage Server Control**.
2. On the **Server Control Policies** tab, select a policy that you want to update.
3. Select **Update**. You can also double-click any policy to update the policy.
4. On the **General** tab, enter a description of the policy in the **Description** field.
5. If the Policy was not finalized, update the policy scripts on the **Policy Script** tab as needed. If the Policy was finalized, select **Create New Version** on the **Policy Script**, and update the policy scripts to create a new version of the policy.
6. Enter appropriate description to provide deployment scripts-specific information in the **Description** field, if needed.
7. Clear the **Finalize** check box to allow further updates to the policy scripts. Select the option to finalize the policy. The default is checked.
8. On the **Version history** tab, all the previous versions of the policy are listed.  
You can select on each version to see the policy script details of that version in the Deploy Script and Undeploy Script sections. You can also select **Download** to download the commands of deploy script and undeploy script of the listed versions, as needed.
9. On the **Policy Dependency** tab, the dependent policies appear under the Members List. Select **OK**. Verify that **Confirmation: PAM-UI-0010: Policy Deleted** appears on the top of the screen.

**NOTE**

You cannot add or remove policies in the existing dependent policies.

**Delete a Server Control Policy**

Do this procedure to delete a Server Control Policy.

**Follow these steps:****NOTE**

Once deleted, you cannot restore a deleted policy. Verify that the following conditions are met before deleting the policies:

- The policy is not dependent on another policy. Remove any dependencies on a policy before you delete the policy.
- All the versions of the policies that are deployed are deleted before you delete a policy.
- The policy is not assigned or deployed on a Server Control Device or Server Control Device Groups.  
Unassign or undeploy the policy from the Server Control Device or Group before you delete the policy.

1. Navigate to **Policies, Manage Server Control**.
2. On the **Server Control Policies** tab, select a policy that you wish to delete.
3. Select **Delete**. Verify that **Confirmation: PAM-UI-0009: Policy Saved** appears on the top of the screen.

**Advanced Server Control Policy Management**

Use advanced policy management functions to manage policies across Server Control devices and device groups by assigning, unassigning, upgrading, and downgrading policies.

To access the advanced policy management functions, navigate to the **Policies, Manage Server Control** screen in the PAM UI. From here you can assign, unassign, deploy, and undeploy policies.

**Assign a Policy**

When you assign a policy, Privileged Access Manager deploys the latest finalized policy version of the stored policy. You can assign a policy on a Server Control device, Server Control device group, or both.

**Follow these steps:**

1. Navigate to **Policies, Manage Server Control** in the PAM UI.  
The **Server Control Policies** page appears.
2. Select a policy that you want to assign and select **Assign/Unassign**.
3. In the **Assign/Unassign Change DS** dialog that opens, move the appropriate device or devices from the **Available Server Control Devices** list to the **Selected Server Control Devices** list.
4. Select **OK**.
5. Select **Yes** to confirm the policy assignment.  
The following message appears at the top of the page: "Policy assign request successfully completed. Check the deployment audit for status"

**Unassign a Policy**

You can unassign a selected policy only on the devices or device groups to which it is assigned. When you unassign a policy, the undeploy policy script is executed. If there is no undeploy policy script, then the deploy policy script is reverted.

**Follow these steps:**

1. Navigate to **Policies, Manage Server Control** in the PAM UI.  
The **Server Control Policies** page appears.
2. Select a policy that you want to unassign and select **Assign/Unassign**.
3. In the **Assign/Unassign Change DS** dialog that opens, move the appropriate device or devices from the **Selected Server Control Devices** list to the **Available Server Control Devices** list.
4. Select **OK**.
5. Select **Yes** to confirm the policy unassignment.  
The following message appears at the top of the page: "Policy UnAssign request successfully completed. Check the Deployment Audit for status."

**Upgrade a Policy**

Upgrade a policy to set it to its latest finalized version on defined hosts. You can only upgrade a policy on a device if a higher version of the policy exists. When you perform the upgrade function on a device, the lower version of the policy is undeployed and the higher version of the policy is deployed.

**TIP****Example:**

Consider you have two versions of a finalized policy Policy\_1 - Policy\_1#1, Policy\_1#2, and the latest finalized policy version, that is Policy\_1#2, is deployed on a Server Control device.

You have updated the policy Policy\_1 which results in a new finalized policy version, that is Policy\_1#3.

To deploy Policy\_1#3 on the mentioned Server Control device, you must perform an upgrade function. When you upgrade the policy on the Server Control device, Policy\_1#2 is undeployed and Policy\_1#3 is deployed.

**Follow these steps:**

1. Navigate to **Policies, Manage Server Control** in the PAM UI.  
The **Server Control Policies** page appears.
2. Select a policy that you want to upgrade and select **Upgrade**.  
The **Upgrade Policy Change** dialog appears.
3. Optionally, filter the available Server Control devices using the **Device Group** field or the search (magnifying glass) icon below it.
4. Select the devices or groups that you want to upgrade from the **Available Server Control Devices** list and move them to **Selected Server Control Devices** list.

5. Select **OK**.
6. Select **Yes** to confirm the policy upgrade.  
The following message appears at the top of the page: "Policy Upgrade request successfully completed. Check the Deployment Audit for status."

### **Downgrade a Policy**

Downgrade a policy to set a specified policy version on defined hosts. You can only downgrade a policy on a device if a lower version of the policy exists. When you downgrade a policy, the higher version of the policy is undeployed and the lower version of the policy is deployed.

#### **TIP**

#### **Example:**

Consider you have two versions of a finalized policy Policy\_1-Policy\_1#1, Policy\_1#2, and the latest finalized policy version, that is Policy\_1#2, is deployed on a Server Control device.

To re-deploy Policy\_1#1 on the mentioned Server Control device, you must perform a downgrade function. When you perform the downgrade function on the Server Control device, Policy\_1#2 is undeployed and Policy\_1#1 is deployed.

#### **Follow these steps:**

1. Navigate to **Policies, Manage Server Control** in the PAM UI.  
The **Server Control Policies** page appears.
2. Select a policy that you want to downgrade and select **Downgrade**.
3. Select the version to which you want to downgrade from the **Policy Versions** drop-down.  
The Server Control Devices on which you can downgrade this policy are listed under **Available Server Control Devices**.
4. Select the devices from the **Available Server Control Devices** list and move them to **Selected Server Control Devices** list.
5. Select **OK**.
6. Select **Yes** to confirm the policy downgrade.  
The policy is downgraded.

## **Server Control Policy Management APIs**

This topic describes the Server Control policy management APIs.

1. Enable and configure the API Docs. See [Use the External REST API \(Programmers\)](#) for details.
2. Select **Settings, API Doc** to access the API Docs.
3. Navigate to **serverControlAccessPolicies** to see a list of available Server Control APIs, implementation notes, parameters, response message, and test API requests.

## **Configure Login Integration for a Server Control Endpoint**

PAM Integrated Server Control supports login integration (auto login) for endpoints connected to Utility Appliances (UAs) and those still connected to legacy Distribution Servers (DSs).

Utility appliances allow PAM to support login integration and access control policy management. To use the PAM access control policy management features, migrate your PIM or PAM SC environment to PAM release 4.0 or later.

As a security administrator, you want to audit the actual user of your server, not the shared local privileged user name. Using PAM Integrated Server Control, login integration integrates the login process and user information. When activated, it allows the use of the actual user name for auditing in PAM Integrated Server Control.



The topics in this section describe how to configure login integration in detail.

**Use the table of contents to access the topics in this section.**

## Agent Status Interval

This content describes how to check the status interval for Agents (endpoint devices) using PAM Integrated Server Control.

**Follow these steps:**

1. To view the status of the device agents, navigate to **Devices, Device Agent Status** to view all agents for Server Control, UNAB, and PUPM devices.
  2. Use the agent status interval settings to show agent status, and filter the devices on the Agent Status panel.
- **Warning Status Interval:** The amount of time expired since the last heartbeat was received by PAM before a warning state is set for the agent on a device.
  - **Failure Status Interval:** The amount of time expired since the last heartbeat was received by PAM before a failure state is set for the agent on a device.
  - **Enable Legacy Login Integration:** Use this option when configuring (or maintaining) *existing* legacy DS systems configured in previous PAM versions. PAM continues to support using the legacy integration but without the access control policy management features. This configuration setting is not applicable to new Distribution Server systems.

## Configure Server Control Login Settings

Complete the following procedures to configure Server Control Login settings:

In general, integrating Server Control Login requires configuring specific Server Control settings and creating the following endpoint definitions:

- Device
- Account
- Application
- Policy

Complete the procedures in this section to configure Server Control Login settings. **Use the table of contents to access the procedures.**

### NOTE

To use server names instead of IP addresses, verify that DNS Servers are configured in the Network Configuration section. In the PAM UI, select **Configuration, Network, Network Settings**. Verify that a DNS IP address is listed in the **DNS Servers** field. If no DNS IP address appears, add your DNS Servers. Select **Update** to save the changes.

## Configure ActiveMQ for Server Control

If you migrated from a legacy PIM or PAM SC environment, you must configure ActiveMQ using the procedure outlined in this content.

### NOTE

This procedure requires information from the Server Control setup.

**Follow these steps:**

1. Log in to the PAM UI.
2. Select **Configuration, Server Control**.



3. Set the **Enable Login Integration** option.
4. In the **ENTM Host Name or IP** field, enter the target server hostname or IP address.
5. Enter the **Port** number, or accept the default 61616.
6. Optionally, unset the **Use SSL** option, which is set by default.
7. Enter the **ActiveMQ Broker Account**. The default is "reportserver."
8. Enter the **Password**.
9. Optionally, specify a different **Message time-to-live** value. The default is 60 minutes.
10. Optionally, specify a different **Reply Timeout**. The default is 10 seconds.
11. Select **Ping AMQ Console** when complete.
12. Verify that your information is correct, and then select **Save**.

## Create PAM Devices for Server Control Endpoints

Create PAM devices to represent endpoint devices on which the user runs the login integration.

Create PAM devices to represent endpoint devices on which the user runs the login integration.

The user needs the device, application, and account so the end user can create an access policy for the login integration to go through. Use the following procedure to create a device for a Server Control endpoint.

### Follow these steps:

1. Select **Devices, Manage Devices**.
2. Select **Add** to create a device.
3. Enter the host name in the **Name** field.
4. Enter the IP address in the **Address** field. To verify the IP address, select **Scan**.
5. Specify the target **Operating System**.
6. Set the **Password Management** option.
7. Select the **Access Methods** tab and select the plus sign (+) Button to add an Access Method.
8. Select the access type (such as SSH or RDP) from the **Name** drop-down list. Specific access method details appear. Add or alter the information as necessary.
9. All other fields on all tabs are optional.
10. Select **OK** to save your changes.

## Create an Application for Server Control Endpoints

The user needs the device, application, and account so the end user can create an access policy for the login integration to go through. Use the following procedure to create an Application for the Privileged Access Manager Server Control endpoint.

The user needs the device, application, and account so the end user can create an access policy for the login integration to go through. Use the following procedure to create an application for the Privileged Access Manager Server Control endpoint.

### Follow these steps:

1. Select **Credentials, Manage Targets, Applications**.
2. Select **Add** to create an application.
3. In the **Host Name** field, either enter the host name, or use the magnifying glass icon to the right of the field to select an existing Device.
4. Enter the **Device Name**. You can also select an existing device using the magnifying glass icon to the right of the **Host Name** field.

5. Enter the target **Application Name**.
6. Select the **Application Type**. If nothing else applies, select **Generic**. Certain Application Types display more options when selected. For example, Windows Proxy allows selection of Local or Domain Account. Most fields are optional or show a default value.
7. Select **OK** to save your changes.

#### NOTE

Windows or Windows-proxy applications using a local account require that you do one of the following steps:

- Use the target device's machine name (netbois name) in the **Address** field of the target device.
- If you use an IP address in the **Address** field, create a selang user for the target account manually: IP\_Address\target\_account.

## Create an Account for Server Control Endpoints

Create an Account for the Privileged Access Manager Server Control endpoint.

#### Follow these steps:

1. Select **Credentials, Manage Targets, Accounts**.
2. Select **Add** to create an account.
3. In the **Host Name** field, either enter the host name in the Host Name field, or use the magnifying glass icon to the right of the field to select an existing Device.
4. Enter the **Device Name**. You can select an existing device using the Select magnifying glass icon to the right of the **Host Name** field.
5. Use the magnifying glass icon to the right of the **Application Name** field to select Applications that have already been created for the Device. Alternatively, use the Add Target Application plus sign (+) icon to add an application directly from this screen.
6. Enter the **Account Name** to use for connecting to the Server Control endpoint.
7. Enter the **Password** for the Account Name that you selected.
8. Other fields are optional. At this point, you may want to enable password management options. For more information, see [Implementing Credential Manager](#).
9. Select **OK** to save your changes.

## Create an Access Policy for Server Control Endpoints

Create an Access Policy for the Server Control host.

#### Follow these steps:

1. Select **Policies, Manage Policies**.
2. Select the **Add** button to create a policy.
3. Select the **User** to use for connecting to the Server Control device.
4. Select the Server Control **Device**.
5. On the **Access** tab, select one or more entries from the **Available Access** list, and then move them to the **Selected Access** list.
6. On the **Symantec PAM Server Control** tab, set the **Login Integration** option.
7. Other fields are optional.
8. Select **OK** to save your changes.

## Test the Login Integration for Server Control Endpoints

To test the Privileged Access Manager Server Control Login Integration, you connect through the Access link on the Access Management page and verify the user name substitution.

### Follow these steps:

1. In the PAM UI, select **Access**. A list of Device Names appears with corresponding Access Methods and Target Applications.
2. Select the **Access Method** link (such as RDP or SSH) for the Server Control Device you are integrating. An RDP or SSH session opens to the Device.
3. For Windows RDP, open PowerShell or the Command prompt. For Linux, use the SSH prompt. The prompt includes the local Server Control privileged user login, not the Privileged Access Manager user.
4. For Windows, enter `secons -whoami`. For Linux, enter `/opt/CA/AccessControl/bin/sewhoami -a`. The Server Control `secons` utility writes several lines of text.
5. Find the "PUPM User" from the output of the previous command. This output should be the Privileged Access Manager user, not the local Server Control privileged user.

### IMPORTANT

Login Integration between PIM 12.x and PAM 4.0 is not supported.

## Change the ActiveMQ Password

The ActiveMQ password is meant for managing the ActiveMQ password on PAM. By default, when PAM is deployed the password is N0tall0wed.

ActiveMQ sends messages between the PAM server and agents running on endpoints. The ActiveMQ section allows the PAM server to either use the default ActiveMQ password, or enter a new password used by all endpoints. This password must match the one used by your endpoints: it does not override or replace an endpoint's existing password.

### NOTE

The Server Control Administrator and Configuration manager roles can see (view) the ActiveMQ section; However, these roles cannot change any fields.

To update the ActiveMQ password, the user should be Server Control Administrator, Configuration Manager, and Password Manager. For the Password Manager role, the user needs to be associated with the ActiveMQ Credential Manager Group; the Credential Manager Group is installed by default, and comes out-of-the-box. The superuser, as always, can also change these options.

### To change the ActiveMQ password, follow either one these steps:

1. Log in to the PAM UI.
2. Select **Configuration, Server Control**.
  - Selecting **Use Default** means the PAM server uses the default ActiveMQ password, which is N0tall0wed
  - To use a uniform, universal password for all your devices, make sure to clear the **Use Default** option, and either enter a new password, or accept the default in the text fields. The default is N0tall0wed.

### NOTE

If you enter a password, the Use Default option becomes unavailable.

## Import PIM and PAM SC Active Directory Users into PAM

Do the following procedure to import PIM and PAM SC Active Directory users into PAM.

**Follow these steps:**

1. In the PAM UI, select **Devices, Manage Devices**. A list of configured devices is displayed.
2. Select **Add**. The **Add Device** page is displayed.
3. Enter the details of the Active Directory server:
  - **Name**: The Active Directory server name
  - **Address**: The Active Directory IP address
  - **Description**: Optionally, provide a description for the device.
  - **Device Type**: Set the **Password Management** option.
4. Select **Save and Add Target Applications**. The **Add Target Application** page is displayed.
5. On the **Add Target Application** page that opens, complete the following details:
  - **Application Name**: The application name
  - **Application Type**: Active Directory
6. Select the **Active Directory** tab and complete the following details:
  - **Domain Name**: *AD\_Domain\_name*
  - **Domain Controller Port (SSL)**: 389
  - **Groups**: Domain Users
7. Navigate to **Credentials, Manage Targets, Accounts**. The **Target Accounts** page is displayed with the list of already existing accounts.
8. Select **Add**. The **Add Target Account** page is displayed.
9. On the **Add Target Account** page that opens, enter the following details:
  - **Host Name**: The IP address of the Active Directory server
  - **Device Name**: The Name of the Device Created Earlier
  - **Application Name**: The Name of the Application Created Earlier
  - **Account Name**: The Name of an AD User who is a member of the Domain Admins Group
  - **Password**: An Active Directory User Password
10. Select the **Active Directory** tab and enter the Distinguished Name.
11. Navigate to **Configuration, 3rdParty, LDAP**. Verify that the AD domain that you added previously is listed.
12. Double-click the domain and verify that all the details are correct.
13. Log in to the PAM UI through the PAM client.
14. Select **Users, Manage User Groups**, and then select **Import LDAP Groups**.
15. In the **Select LDAP domain** dialog that opens, select the AD domain that you added previously and click **OK**.
16. Select the required groups and select **Register selected groups with the PAM appliance**.
17. Select **Register groups**. The selected groups are registered.
18. Go to **Users, Manage Users** and verify that all the imported AD users are displayed.

## Configure UNAB to Provide Access to UNIX Computers Using Active Directory

The content in this section describes how to configure UNAB to provide access to UNIX systems using an Active Directory data store.

**NOTE**

In contrast to PIM and PAM SC, PAM 4.0 does not support manually creating either UNAB users or UNAB user groups. PAM 4.0 also does not support creating a Login Authorization Policy for UNAB users or UNAB user groups. You can only use LDAP to import Users or User Groups. For more information, [Import LDAP User Groups](#) and [Import LDAP Device Groups](#).

Use the table of contents to access the topics in this section.

## UNIX Authentication Broker (UNAB) Overview

This content provides an overview of the UNIX Authentication Broker (UNAB).

### UNAB Components

The UNIX Authentication Broker (UNAB) consists of several components that manage and control access to the UNIX host by Active Directory users.

- **UNAB authentication agent:** The UNAB authentication agent (uxauthd) daemon services the connection with Active Directory. The agent has the following responsibilities, among others:
  - Maintaining a secure connection with Active Directory for user authentication and login authorization purposes
  - Host registration with Active Directory
  - User and group migrations
  - Administering the local access files
- **uxconsole:** The uxconsole is the UNAB management console. Use the console to register the UNIX host with Active Directory, migrate users and groups, and to register and activate UNAB.
- **Privileged Access Manager Server Control Enterprise Management:** This component lets you manage your UNAB hosts from a central location. Using Privileged Access Manager Server Control Enterprise Management, you can:
  - Control Active Directory users access to every UNAB host in the enterprise.
  - Manage hosts login authorizations.
  - Resolve hosts migration conflicts.
  - Generate reports

### How To Set up UNAB

Understanding how the UNIX Authentication Broker (UNAB) controls access to the UNIX host provides you with information that helps you during the implementation and configuration process. After you install UNAB on the UNIX host, register UNAB with Active Directory. Activate UNAB to enable enterprise users to authenticate to UNIX endpoints. You then begin the migration process to migrate local users and groups in to Active Directory.

1. Register the UNIX host with Active Directory.  
At this stage UNAB does not intercept any login requests.
2. Define which enterprise users and groups are permitted or denied access to the UNIX host. You do so by creating login authorization policies from **Privileged Access Manager Server Control Enterprise Management**.
3. Activate UNAB to enable enterprise users authentication to the UNIX host.
4. Add more enterprise users and groups to the UNAB login authorization policies to enable new users to log in.  
At this stage, users who are defined in the local user store (for example, etc/passwd) and enterprise users who are permitted by UNAB login authorization policies can log in.
5. Migrate users and groups into Active Directory.

### How UNAB Authenticates Users

After you install and configure UNAB on the UNIX host, users can log in with their Active Directory user account or their local user account, according to the integration mode you implemented. When a user attempts to log in to a UNIX host where UNAB is running, the following events occur:

1. The user is prompted for an Active Directory or local account user name and password.
2. UNAB authenticates the user credentials with Active Directory, using the login authorization policy or the local host access files. UNAB also checks for additional information that is taken from the user account.
3. If the user is authenticated, UNAB grants the user access to the UNIX host. If not, UNAB blocks the user access to the host.

## Information Stored on the UNAB Endpoint

After UNAB authenticates a user, UNAB stores the following information about the endpoint:

- User name
- Hashed password (using SHA-2)
- User class attributes
- User account control
- Time of the last good login
- Time of the last bad login
- Number of bad logins since last good login

UNAB saves the user details in the `logon.db` file. The NSS database saves the user and groups attributes in the `nss.db` file. Both files reside in the directory `/opt/CA/uxauth/etc`.

## Manage UNAB Login Authorization for Devices and Device Groups

The content in this section describes how to manage UNAB login authorization for devices and device groups, most of which occurs on the **UNAB Login Authorization Policies** panel.

### NOTE

Unlike PIM and PAM SC, Integrated PAM SC does not support manually creating UNAB users or UNAB user groups. Integrated PAM SC also does not support creating a Login Authorization Policy for UNAB users or UNAB user groups. You can only use LDAP to import Users or User Groups. For more information, [Import LDAP User Groups](#) and [Import LDAP Device Groups](#).

- [Add a UNAB User Login Authorization to Devices](#)
- [Add a UNAB Config Token to a Device Group](#)
- [Add UNAB User Group Login Authorization to a Device](#)
- [Add a UNAB User Group Login Authorization to a Device Group](#)
- [Update the UNAB User Login Authorization Policy for a Device or Device Group](#)
- [Update the UNAB User Group Login Authorization Policy for a Device or Device Group](#)

### TIP

For information about troubleshooting tasks available from the other tabs on the **UNAB Login Authorization Policies** panel, see the following topics:

- [Troubleshoot Policies Deployed on UNAB Devices](#) (**Device Troubleshooting** tab).
- [Troubleshoot Policies Deployed on UNAB Device Groups](#) (**Device Group Troubleshooting** tab).

## Add a UNAB User Login Authorization to Devices

Do the following procedures to add a UNAB user login authorization to devices.

### NOTE

In contrast to PAMSC, PAM 4.0 does not support either manually creating either UNAB users or UNAB user groups, nor creating a Login Authorization Policy for these UNAB users or UNAB user groups. You can only use LDAP to import Users or User Groups. For more information, [Import LDAP User Groups](#) and [Import LDAP Device Groups](#).

## Add Users and User Groups

Do this procedure to add users and user groups.

**Follow these steps:**

1. In the PAM UI, select **Policies, Manage UNAB Policies**. The **UNAB Login Authorization Policies** screen appears.
2. Select **Add**. The **Add UNAB Login Authorization Policy** dialog appears.
3. Add a description for the policy in the **Description** field.
4. Use the **Device Name** tab to select the device to add to the policy.  
The Available Groups list identifies all UNAB Users that exist on this Privileged Access Manager appliance.
5. Use the **Users** tab to select the users or user groups to associate with a policy. The Available Users and Groups lists identify all Active Directory users and user groups that exist and that are linked to a UNAB host machine. These users and user groups are imported from AD/LDAP using the PAM LDAP importer. These users and user groups must have a CA ControlMinder attribute to appear in the **Login Authorization** policy page.
6. Select the desired user or user group, and then select **OK**.

**Add Users to Policies**

Do this procedure to add users to policies.

**Follow these steps:**

1. In the PAM UI, select **Policies, Manage UNAB Policies**. The **UNAB Login Authorization Policies** screen appears.
2. From the **UNAB Login Authorization Policies** tab, select the policy to update, and then select **Update**.  
The **Update UNAB Login Authorization Policy** dialog appears.
3. Select the **Users** tab and use the shuttle to select users for your policy.
4. Select **OK** to confirm the change and exit this dialog.

**Add User Groups to Policies**

Do this procedure to add user groups to policies.

**Follow these steps:**

1. In the PAM UI, select **Policies, Manage UNAB Policies**. The **UNAB Login Authorization Policies** screen appears.
2. From the **UNAB Login Authorization Policies** screen, select the policy to update, and then select **Update**.  
The **Update UNAB Login Authorization Policy** dialog appears.
3. Select the **User Groups** tab and use the shuttle to select user groups for your policy.
4. Select **OK** to confirm the change and exit this dialog.

**Audit UNAB Policy Deployments**

You can audit your UNAB policy deployments. This audit gives you a view of your UNAB policy deployments and a descriptive list of deployment tasks. The list details what triggered each deployment task, when it was created, and what type of deployment was involved. For each deployment task, you can further explore the following details:

- For which host and policy pair the deployment task created
- The version of the policy that was deployed
- The status of the deployment task (queued, succeeded, or failed)
- The `selang` output (result of deploying the command)

**To audit UNAB policy deployments, follow these steps:**

1. In the PAM UI, select **Policies, Manage UNAB Policies**. The **UNAB Login Authorization Policies** screen appears.
2. In the **UNAB Login Authorization Policies** screen, select **Deployment Audit**. The **Deployment Audit** dialog appears.



3. Define a scope for the deployment audit using the Column and Value filters, and then select **View**. To view the policy, the user selects a particular policy and then selects **View**. The Privileged Identity Manager Enterprise Console retrieves information about deployments that are in the scope you defined and displays the results after a short delay.

## Add a UNAB Config Token to a Device Group

Do this procedure to add a UNAB Configuration Token to a device group.

### Follow these steps:

1. In the PAM UI, select **Devices, Manage Devices, Groups**.  
A list of all devices groups is displayed.
2. Select the UNAB device group and double-click or click on **Update**.  
The **Update Device** page is displayed.
3. Click on the **UNAB** tab. The current **UNAB Configuration Token Update** page is displayed.
4. Click on the **+** icon.  
A new blank row is displayed.
5. Select the appropriate section, token, and value from the drop-down menu and click **OK**.

## Add UNAB User Group Login Authorization to a Device

Use the following procedure to add a UNAB User Group Login Authorization to a device.

1. In the PAM UI, select **Policies, Manage UNAB Policies**.  
The **UNAB Login Authorization Policies** tab appears.
2. From the **UNAB Login Authorization Policies** tab, select **Add**.  
The **Add UNAB Login Authorization Policy** window appears.
3. Add a description for the policy in the **Description** field.
4. Use the **Device Name** tab to select the device to add to the policy.
5. Use the **User** tabs to select the User Group to associate with a policy.  
The Available Users and Groups lists identify all Active Directory users and Groups that exist and are linked to a UNAB host machine. These users and user groups are imported from AD/LDAP using the PAM LDAP importer. These users and user groups must have a CA ControlMinder attribute to appear in the Login Authorization policy page.
6. Select the desired user, and then select **OK**.

## Add a UNAB User Group Login Authorization to a Device Group

This procedure describes how to add a UNAB User Group Login Authorization to a Device Group:

### Follow these steps:

1. In the PAM UI, select **Policies, Manage UNAB Policies**.  
The UNAB Login Authorization Policies tab appears.
2. From the **UNAB Login Authorization Policies** tab, select **Add**.  
The **Add UNAB Login Authorization Policy** window appears.
3. Add a description for the policy in the **Description** field.
4. Use the **Device Name** tab to select the device group to add to the policy.  
The Available Groups list identifies the UNAB users that exist on this Privileged Access Manager appliance.
5. Use the **User** tab to select the user group to associate with a policy.



The Available Users and Groups lists identify the Active Directory users and groups that exist and that are linked to a UNAB host machine. These users and user groups are imported from AD/LDAP using the PAM LDAP importer. These users and user groups must have a CA ControlMinder attribute to appear in the Login Authorization policy page.

6. Select the desired user, and then select **OK**.

## Update the UNAB User Login Authorization Policy for a Device or Device Group

This procedure describes how to update the UNAB User login authorization policy for a device or device group.

### Follow these steps:

1. In the PAM UI, select **Policies, Manage UNAB Policies**.  
The **UNAB Login Authorization Policies** tab appears.
2. From the **UNAB Login Authorization Policies** tab, select the policy and then select **Update**.  
The **Update UNAB Login Authorization Policy** window appears.
3. Select the **Users** tab.
  - Use the shuttle to select users for your policy.
  - Select **OK** to confirm the changes and exit this window.

## Update the UNAB User Group Login Authorization Policy for a Device or Device Group

This procedure describes how to update the UNAB User Group Login Authorization Policy for a device or device group.

### Follow these steps:

1. In the PAM UI, select **Policies, Manage UNAB Policies**.  
The **UNAB Login Authorization Policies** tab appears.
2. From the **UNAB Login Authorization Policies** tab, select the policy and then select **Update**.  
The **Update UNAB Login Authorization Policy** window appears.
3. Select the **Users Groups** tab.
  - Use the shuttle to select groups for your policy.
  - Select **OK** to confirm the changes and exit this window.

## Configure a UNAB Host or Host Group

Use these procedures to configure a UNAB host or host group.

This page contains the following topics:

### Add a UNAB Configuration Token to a Device

Do this procedure to add a UNAB Configuration Token to a device.

### Follow these steps:

1. In the PAM UI, select **Devices, Manage Devices**.  
A list of all devices appears.
2. Select the UNAB device, and then select **Update**.  
The **Update Device** page appears.
3. Select the **UNAB** tab. The current **UNAB Configuration Token Update** page appears.
4. Select the **+** icon. A new blank row appears.
5. Select the appropriate section, token, and value from the drop-down menu.
6. Select **OK**.

## **Add a UNAB Configuration Token to a Device Group**

Do this procedure to add a UNAB Configuration Token to a device group.

### **Follow these steps:**

1. In the PAM UI, select **Devices, Manage Device Groups**.  
A list of all devices groups appears.
2. Select the UNAB device group and then select **Update**.  
The **Update Device** page appears.
3. Select the **UNAB** tab. The current **UNAB Configuration Token Update** page appears.
4. Select the **+** icon.  
A new blank row appears.
5. Select the appropriate section, token, and value from the drop-down menu, and select **OK**.

## **Verify Policy Deployment from a UNAB Endpoint**

Do this procedure to verify policy deployment from a UNAB endpoint.

### **Follow these steps:**

1. In the PAM UI, go to **Policies, Manage UNAB Policies, Deployment Audit**.  
All deployed policies are listed.
2. Double-click on any of the policies to view its status. The details of the deployed policy appear in the box.
3. Verify that a successfully deployed login authorization policy has taken effect in the UNAB endpoint:
  - a. Log in to the UNAB endpoint.
  - b. Run the following UNAB command to verify the deployed login authorization policy. Replace <user name> with the name of an AD user.  
`uxconsole -manage -show -user <user name>`
  - c. If the login authorization policy is successfully deployed, the AD user is allowed to log in. The login reason displays as **"According to login policy."**
  - d. Log in to the UNAB endpoint as this AD user. The user is allowed to log in.
4. Verify that a successfully deployed config policy has taken effect in the UNAB endpoint:
  - a. Log in to the UNAB endpoint.
  - b. Access the `/opt/CA/uxauth/uxauth.ini` and `/opt/CA/AccessControlShared/ acccommon.ini` files and verify if the configuration changes appear.
  - c. Cross-check the values of the token, based on the config policy deployed from the PAM UI.

## **Manage Server Control UNAB Policies Using the PAM External API**

This content describes how to use the External API documentation to learn how to manage Server Control policies using the PAM external API.

This page contains the following topics:

### **Find Policy Information**

1. In the PAM UI, navigate to **Settings, API Doc**.
2. Go to **servercontrolUNABPolicies**.
3. Select **GET/PUT/POST** and select **Try it out**. The appropriate policy information appears (GET) or the policy updates (PUT or POST).

### **Finding Device Config Policy**

1. In the PAM UI, navigate to **Settings, API Doc**.
2. Select **Devices**.
3. Select GET /api.php/v1/devices.json/{id}/unabConfig
4. Enter a valid device ID and select **Try it out**. The config policies deployed on the device appear.

### **Finding Device Group Config Policy**

1. In the PAM UI, navigate to **Settings, API Doc**.
2. Select **deviceGroups**.
3. Select GET /api.php/v1/deviceGroups.json/{id}/unabConfig.
4. Enter a valid device group ID and select **Try it out**. The deployed config policies in the device group appear.

## **TIBCO Configuration in PAM**

Complete these procedures to set up a TIBCO configuration in PAM to support older PIM Agents. You must have configured a Utility Server for your PAM implementation before you begin. See [Download and Deploy a Utility Appliance](#) for procedures.

1. In PAM, navigate to **Configuration, Utility Appliance Patches, Available Patches**.
2. Click **Upload**. In the Upload utility appliance dialog box, choose the TIBCO patch file and click **Upload**  
The TIBCO patch appears under **Available Patches**.
3. Click the TIBCO patch and select **Stage**. A confirmation message appears, stating that the Utility Appliance Patch stage process has initiated.
4. Navigate to the Patch level tab. The TIBCO patch appears without a version number.
5. Select the TIBCO patch and click **Update**.
6. In the Change Utility Appliance Version dialog box, select the version to which the patch should be updated and click **OK**.  
A confirmation message appears stating that the item was saved, and the TIBCO patch appears with the updated version number.

## **Administrate PAM SC**

This section describes how to do PAM Server Control administration functions.

**Use the table of contents to access the topics in this section.**

### **Endpoint Administration for UNIX**

This section describes UNIX endpoint management tasks and concepts.

- [Manage Endpoints](#)
- [Safe User Substitution](#)
  - [Define SUDO Records](#)
- [Prevent Password Attacks](#)
- [Restrict Access to Files and Directories](#)
- [Synchronization with Native UNIX Security](#)
- [Monitor Sensitive Files](#)
- [Protect setuid and setgid Programs](#)
- [Kernel Modules Load and Unload Protection](#)

- Protect Binary Files from the kill Command
- Control Login Commands
- Protect TCP/IP Services
- The Policy Model Database
- Dual Control
- Use the seagent and sepmdd Daemons
- Protect Idle Stations
- Protect Resources Using APIs
- Protect Against Stack Overflow STOP
- Security Levels
- Security Categories
- Security Labels
- Audit Logs (UNIX)
- Log Routing
- Migrate User Trace Filters
- Improve Performance
- UNIX Exits
- Interact with LDAP
- NIS Configuration

## Manage Endpoints

Privileged Access Manager is a software product that is an active, comprehensive security software solution for Open Systems, tied dynamically to the operating system. Each time a user requests a security-sensitive operation, such as opening a file, substituting a user ID, or obtaining a network service, the product can intercept the event in real time. The product can evaluate the validity of the operation before passing control to the standard operating system (OS) functions.

Privileged Access Manager provides two ways to manage the resources in your enterprise and control who has access to them:

- **selang:** the Privileged Access Manager command language.  
The selang command language lets you make definitions in the Privileged Access Manager database. The selang command language is the command definition language.  
**Note:** For more information about using selang, see the *selang Reference* section.
- **Privileged Access Manager Endpoint Management:** the endpoint administration interface.  
The web-based interface lets you administer remote endpoints through a central administration server.  
**Note:** For more information about installing Privileged Access Manager Endpoint Management, see the *Implementation* section.

This article contains the following sections:

### About Privileged Access Manager

Privileged Access Manager provides you with a powerful tool for managing security for your native platforms. The product makes it possible to implement a security policy that you customize to the security requirements of the enterprise. Privileged Access Manager lets you provide security for users, groups, and resources beyond what is available in native operating systems. It lets you centrally manage security across the organization and integrate your Windows and UNIX security policies in a heterogeneous environment.

### **Why Does UNIX Need Protecting?**

Many operating systems have built-in access control, using one technique or another. IBM z/OS, a well-established and mature mainframe operating system, includes the System Authorization Facility (SAF). SAF is a set of calls that the operating system issues to verify the authorization of a user.

Access control software in a z/OS environment sets a return code for the SAF call and z/OS grants or denies access according to the code. The decision of what return code to set is based on the access rules and policies defined in the security database by the security administrator.

Other operating systems, such as OS/2, provide similar techniques for access control. The OS/2 access control module, named Security Enabling Services (SES), is based on the same concept as z/OS SAF.

Unfortunately, UNIX-based operating systems were not designed this way. Authorization decisions are made mainly for file accesses. The operating system performs these decisions using the 9 bits (rwx-rwx-rwx) in the *inode* entry of the file. Unlike SAF, no exit point for event interception is provided. Therefore, further security is necessary to perform functions that are more complex than those functions of mainframe-type security packages.

### **What is Protected?**

#### **Valid on UNIX**

In addition to supplying the regular security functions such as an access rule database, an audit log, and administration tools, Privileged Access Manager intercepts the operating system events that are to be protected. Because Privileged Access Manager works with many different operating systems, it intercepts events in memory. No changes are made to system files, and the operating system is not modified.

Privileged Access Manager protects the following entities:

- **Files**

Is a user authorized to access a particular file?

Privileged Access Manager restricts the ability of a user to access a file. You can give a user one or more types of access, such as READ, WRITE, EXECUTE, DELETE, and RENAME. You can specify the access to an individual file or to a set of similarly named files.

- **Terminals**

Is a user authorized to use a particular terminal?

This check is done during the login process. Individual terminals and groups of terminals can be defined in the Privileged Access Manager database, with access rules. These rules determine which users, or groups of users, are allowed to use the terminal or terminal group. Terminal protection ensures that no unauthorized terminal or station is used to log in to the accounts of powerfully authorized users.

- **Sign-on time**

Is a user authorized to log in at a particular time on a particular day?

Most users use their stations only on weekdays and only during work hours. The time-of-day and day-of-week login restrictions, and holiday restrictions, provide protection from hackers and from other unauthorized accessors.

- **TCP/IP**

Is another station authorized to receive TCP/IP services from the local computer? Is another station authorized to supply TCP/IP services to the local computer? Is another station permitted to receive services from every user of the local station?

An open system is a system in which both the computers and the networks are open. The advantage of an open system is also a disadvantage. Once a computer is connected to the outside world, one can never be sure who enters the system and what damage an alien user may do, intentionally or by mistake. Privileged Access Manager includes firewalls that prevent local stations and servers from providing services to unknown stations.

- **Multiple login privileges**

Is the user permitted to log in from a second terminal?

The term *concurrent logins* refers to the ability of a user to log in to the system from more than one terminal. Privileged Access Manager can prevent a user from logging in more than once. This protection prevents intruders from logging in to the accounts of users who are already logged in.

- **User-defined entities**

You can define and protect both regular entities (such as TCP/IP services and terminals) and functional entities. Functional entities are known as *abstract* objects, such as performing a transaction and accessing a record in a database.

- **Aspects of administrator authority**

Privileged Access Manager provides the means to both delegate superuser authorities to operators and restrict the permissions of the superuser account.

- **Substitute-user**

Are users authorized to substitute their user IDs?

The UNIX *setuid* system call is one of the most sensitive services that are provided by the operating system. Privileged Access Manager intercepts this system to determine whether the user is authorized to perform the substitution. The substitute-user authority check includes program pathing—users are permitted to substitute their user IDs only through specific programs. This check is especially important in controlling who can substitute to root and therefor gain root access.

- **Substitute-group**

Is a user authorized to issue the *newgrp* (substitute-group) command?

Substitute-group protection is similar to substitute-user protection.

- **Setuid and setgid programs**

Can a particular *setuid* or *setgid* program be trusted? Is the user authorized to invoke it?

The security administrator can test programs that are marked as *setuid* or *setgid* executables to ensure that they do not contain any security loopholes that can be used to gain unauthorized access. Programs that pass the test and are considered safe are defined as trusted programs. The Privileged Access Manager Self-Protection Module (also referred to as the Privileged Access Manager *watchdog*) knows which program is in control at a particular time. The module checks whether the program has been modified or moved because it was classified as trusted. If a trusted program is modified or moved, the program is no longer considered trusted and Privileged Access Manager does not allow it to run.

In addition, Privileged Access Manager protects against various deliberate and accidental threats, including:

- **Kill attempts**

Protects critical servers and services or daemons against kill attempts.

- **Password Attack**

Protects against various types of password attacks, enforces the password-definition policies of your site, and detects break-in attempts.

- **Password Delinquency**

Delineates rules that force users to create and use passwords of sufficient quality. To ensure that users create and use acceptable passwords, Privileged Access Manager can set maximum and minimum lifetimes for passwords, restrict certain words, prohibit repetitive characters, and enforce other restrictions. Passwords are not permitted to last too long.

- **Account Management**

Ensures that dormant accounts are dealt with appropriately.

- **Domain Management**

Implements password protection and enforce security across NIS and non-NIS domains.

## About Symantec Privileged Access Manager Server Control

Privileged Access Manager provides a powerful tool for managing security for your native platforms, enabling you to:

- Implement a security policy customized for the requirements of your enterprise.
- Provide security for users, groups, and resources beyond what is available in native operating systems.
- Centrally manage security across the organization and integrate your Windows and UNIX security policies in a heterogeneous environment.

**To access the topics in this section, use the table of contents.**

## Why Does UNIX Need Protecting?

Many operating systems have built-in access control, using one technique or another. IBM z/OS, a well-established and mature mainframe operating system, includes the System Authorization Facility (SAF). SAF is a set of calls that the operating system issues to verify the authorization of a user.

Access control software in a z/OS environment sets a return code for the SAF call and z/OS grants or denies access according to the code. The decision of what return code to set is based on the access rules and policies defined in the security database by the security administrator.

Other operating systems, such as OS/2, provide similar techniques for access control. The OS/2 access control module, named Security Enabling Services (SES), is based on the same concept as z/OS SAF.

Unfortunately, UNIX-based operating systems were not designed this way. Authorization decisions are made mainly for file accesses. The operating system performs these decisions using the 9 bits (rwx-rwx-rwx) in the *inode* entry of the file. Unlike SAF, no exit point for event interception is provided. Therefore, further security is necessary to perform functions that are more complex than those functions of mainframe-type security packages.

## What Is Protected

### Valid on UNIX

In addition to supplying the regular security functions such as an access rule database, an audit log, and administration tools, Privileged Access Manager intercepts the operating system events that are to be protected. Because Privileged Access Manager works with many different operating systems, it intercepts events in memory. No changes are made to system files, and the operating system is not modified.

Privileged Access Manager protects the following entities:

- **Files**

Is a user authorized to access a particular file?

Privileged Access Manager restricts the ability of a user to access a file. You can give a user one or more types of access, such as READ, WRITE, EXECUTE, DELETE, and RENAME. You can specify the access to an individual file or to a set of similarly named files.

- **Terminals**

Is a user authorized to use a particular terminal?

This check is done during the login process. Individual terminals and groups of terminals can be defined in the Privileged Access Manager database, with access rules. These rules determine which users, or groups of users, are allowed to use the terminal or terminal group. Terminal protection ensures that no unauthorized terminal or station is used to log in to the accounts of powerfully authorized users.

- **Sign-on time**

Is a user authorized to log in at a particular time on a particular day?

Most users use their stations only on weekdays and only during work hours. The time-of-day and day-of-week login restrictions, and holiday restrictions, provide protection from hackers and from other unauthorized accessors.

- **TCP/IP**

Is another station authorized to receive TCP/IP services from the local computer? Is another station authorized to supply TCP/IP services to the local computer? Is another station permitted to receive services from every user of the local station?

An open system is a system in which both the computers and the networks are open. The advantage of an open system is also a disadvantage. Once a computer is connected to the outside world, one can never be sure who enters the system and what damage an alien user may do, intentionally or by mistake. Privileged Access Manager includes firewalls that prevent local stations and servers from providing services to unknown stations.

- **Multiple login privileges**

Is the user permitted to log in from a second terminal?



The term *concurrent logins* refers to the ability of a user to log in to the system from more than one terminal. Privileged Access Manager can prevent a user from logging in more than once. This protection prevents intruders from logging in to the accounts of users who are already logged in.

- **User-defined entities**

You can define and protect both regular entities (such as TCP/IP services and terminals) and functional entities. Functional entities are known as *abstract* objects, such as performing a transaction and accessing a record in a database.

- **Aspects of administrator authority**

Privileged Access Manager provides the means to both delegate superuser authorities to operators and restrict the permissions of the superuser account.

- **Substitute-user**

Are users authorized to substitute their user IDs?

The UNIX *setuid* system call is one of the most sensitive services that are provided by the operating system. Privileged Access Manager intercepts this system call to determine whether the user is authorized to perform the substitution. The substitute-user authority check includes program pathing—users are permitted to substitute their user IDs only through specific programs. This check is especially important in controlling who can substitute to root and therefore gain root access.

- **Substitute-group**

Is a user authorized to issue the *newgrp* (substitute-group) command?

Substitute-group protection is similar to substitute-user protection.

- **Setuid and setgid programs**

Can a particular *setuid* or *setgid* program be trusted? Is the user authorized to invoke it?

The security administrator can test programs that are marked as *setuid* or *setgid* executables to ensure that they do not contain any security loopholes that can be used to gain unauthorized access. Programs that pass the test and are considered safe are defined as trusted programs. The Privileged Access Manager Self-Protection Module (also referred to as the Privileged Access Manager *watchdog*) knows which program is in control at a particular time. The module checks whether the program has been modified or moved because it was classified as trusted. If a trusted program is modified or moved, the program is no longer considered trusted and Privileged Access Manager does not allow it to run.

In addition, Privileged Access Manager protects against various deliberate and accidental threats, including:

- **Kill attempts**

Protects critical servers and services or daemons against kill attempts.

- **Password Attack**

Protects against various types of password attacks, enforces the password-definition policies of your site, and detects break-in attempts.

- **Password Delinquency**

Delineates rules that force users to create and use passwords of sufficient quality. To ensure that users create and use acceptable passwords, Privileged Access Manager can set maximum and minimum lifetimes for passwords, restrict certain words, prohibit repetitive characters, and enforce other restrictions. Passwords are not permitted to last too long.

- **Account Management**

Ensures that dormant accounts are dealt with appropriately.

- **Domain Management**

Implements password protection and enforces security across NIS and non-NIS domains.

## How Privileged Access Manager Server Control Protects UNIX

Privileged Access Manager starts immediately after the operating system finishes its initialization. Privileged Access Manager places hooks in system services that must be protected. In this way, control is passed to Privileged Access Manager before the service is performed. The product decides whether to grant the service to the user.



For example, a user attempts to access a resource protected by Privileged Access Manager. This access request generates a system call to the kernel to open the resource. Privileged Access Manager intercepts that system call and decides whether to grant access. If permission is granted, Privileged Access Manager passes control to the regular system service. If the product denies permission, it returns the standard permission-denied error code to the program that activated the system call. The system call ends.

The decision is based on access rules and policies that are defined in the database. The database describes two types of objects: accessors and resources. *Accessors* are users and groups. *Resources* are objects to be protected, such as files and services. Each record in the database describes an accessor or a resource.

Each object belongs to a class—a collection of objects of the same type. For example, `TERMINAL` is a class containing objects that are terminals (workstations) protected by Privileged Access Manager.

### **Class Activation**

Privileged Access Manager stores information about whether a `CLASS` is active or inactive in the database. When Privileged Access Manager starts, it passes a list of active classes to `SEOS_syscall`, so Privileged Access Manager does not have to constantly intercept these classes. The only time Privileged Access Manager intercepts a class is when a user changes the activity status of a class. If a class is inactive, access to the resource is not intercepted.

You can use the inactive class bypass with the following classes: `FILE`, `HOST`, `TCP`, `CONNECT`, and `PROCESS`.

### **Accessor Elements**

An *accessor element* (ACEE) represents each user. The accessor element is an in-memory reflection of the record of the user in the database. Privileged Access Manager builds the accessor element during the login process. The accessor element is associated with the process of the user. Whenever the process requests a system service that is protected by Privileged Access Manager, or issues an implicit request to access a resource, the product accesses the record of the resource. The product then determines whether the information in the previously created accessor element, such as the security level of the user, mode, and group—lets the user access the resource.

### **Class Activation**

Privileged Access Manager stores information about whether a `CLASS` is active or inactive in the database. When Privileged Access Manager starts, it passes a list of active classes to `SEOS_syscall`, so Privileged Access Manager does not have to constantly intercept these classes. The only time Privileged Access Manager intercepts a class is when a user changes the activity status of a class. If a class is inactive, access to the resource is not intercepted.

You can use the inactive class bypass with the following classes: `FILE`, `HOST`, `TCP`, `CONNECT`, and `PROCESS`.

### **Accessor Elements**

An *accessor element* (ACEE) represents each user. The accessor element is an in-memory reflection of the record of the user in the database. Privileged Access Manager builds the accessor element during the login process. The accessor element is associated with the process of the user. Whenever the process requests a system service that is protected by Privileged Access Manager, or issues an implicit request to access a resource, the product accesses the record of the resource. The product then determines whether the information in the previously created accessor element, such as the security level of the user, mode, and group—lets the user access the resource.

## **Expanding UNIX Native Security**

The following Privileged Access Manager features expand native security.

## **Superuser Account Limitations**

Users who administer and manage operating systems are typically members of predefined accounts. These accounts are automatically created during the system setup, such as the root account on UNIX systems and the Administrator account on Windows systems. Each of the predefined accounts exists to perform a certain set of system functions.

For example, users acting as root or Administrator can create, delete, and modify users and lock, reconfigure, and shut down servers.

One of the major security risks is that an unauthorized user gains control of these accounts. If this happens, the user can seriously damage the system.

Privileged Access Manager can limit the rights that are granted to these accounts. The product can limit the rights of members of user groups that have these accounts as members. This reduces the vulnerability of your operating system.

## **Privileged Access Manager Administrator**

When you install Privileged Access Manager, you are asked to name one or more Privileged Access Manager administrators. Administrators have the authority to modify all or part of the rules database. You should have at least one full-authority administrator. This administrator can modify or create access rules freely and can designate other levels of administrators.

Once you have defined users for your system, you can assign administrative authority to other users by assigning the ADMIN attribute to them.

**Note:** A user with the ADMIN attribute possesses powerful authority. Consequently, the number of ADMIN users should be strictly limited. It is also a good policy to separate the roles of the native superuser and ADMIN, removing the ADMIN attribute from the superuser after you have set up one or more Privileged Access Manager security administrators.

Because you always need at least one user with authority to manage the database, Privileged Access Manager does not let you delete the last user that has the ADMIN attribute.

If you expect any of the Privileged Access Manager administrators to administer other hosts from this workstation, be sure that a rule in the database on that host gives them READ and WRITE access from this workstation.

## **Sub Administration**

Privileged Access Manager contains a *sub administration* feature. This lets administrators grant specific privileges that enable regular users to manage specific classes. These users are then called sub administrators.

For example, you can allow a specific user to manage users and groups only.

You can also specify a higher level of sub administration by granting access not only for specific classes, but for specified records in these classes.

## **Administration Rights for Regular Users**

Privileged Access Manager lets you grant ordinary users (non-administrators) the rights and privileges to perform administrative tasks without being members of the Administrators group. The ability to delegate tasks by granting administrative privileges in this granular way is a significant advantage of Privileged Access Manager.

- A record in the SUDO class stores a command script to allow users to run the script with borrowed permissions.
- The data property value is the command script. This value can be modified by adding to it optional script parameter values.
- Each record in the SUDO class identifies a command for which a user can borrow permissions from another user.
- The key of the SUDO class record is the name of the SUDO record. This name is used instead of the command name when a user executes the commands in the SUDO record.

## Program Pathing

*Program pathing* is an access rule associated with a file that requires that the file is accessed only through a specific program. Program pathing greatly increases the security of sensitive files. Privileged Access Manager lets you use program pathing to provide additional protection for the files in your system.

## B1 Security Level Certification

Privileged Access Manager includes the following B1 Orange Book features: security levels, security categories, and security labels.

- Accessors and resources in the database can be assigned a *security level*. The security level is an integer from 1 through 255. An accessor can gain access to a resource only if the accessor has a security level equal to or greater than the security level assigned to the resource.
- Accessors and resources in the database can belong to one or more *security categories*. An accessor can access a resource only if the accessor belongs to all of the security categories assigned to the resource.
- A *security label* is a name that associates a particular security level with a set of zero or more security categories. Assigning a user to a security label gives the user both the security level and any security categories that are associated with the security label.

**Note:** For more information about B1 Orange Book features, see the *Implementation* section.

## Superuser Account Limitations (UNIX)

Users who administer and manage operating systems are typically members of predefined accounts. These accounts are automatically created during the system setup, such as the root account on UNIX systems and the Administrator account on Windows systems. Each of the predefined accounts exists to perform a certain set of system functions.

For example, users acting as root or Administrator can create, delete, and modify users and lock, reconfigure, and shut down servers.

One of the major security risks is that an unauthorized user gains control of these accounts. If this happens, the user can seriously damage the system.

Privileged Access Manager can limit the rights that are granted to these accounts. The product can limit the rights of members of user groups that have these accounts as members. This reduces the vulnerability of your operating system.

## UNIX Account Administrative Authority in PAM SC

When you install Privileged Access Manager, you are asked to name one or more Privileged Access Manager administrators. Administrators have the authority to modify all or part of the rules database. You should have at least one full-authority administrator. This administrator can modify or create access rules freely and can designate other levels of administrators.

Once you have defined users for your system, you can assign administrative authority to other users by assigning the ADMIN attribute to them.

### NOTE

A user with the ADMIN attribute possesses powerful authority. Consequently, the number of ADMIN users should be strictly limited. It is also a good policy to separate the roles of the native superuser and ADMIN, removing the ADMIN attribute from the superuser after you have set up one or more Privileged Access Manager security administrators.

Because you always need at least one user with authority to manage the database, Privileged Access Manager does not let you delete the last user that has the ADMIN attribute.

If you expect any of the Privileged Access Manager administrators to administer other hosts from this workstation, be sure that a rule in the database on that host gives them READ and WRITE access from this workstation.

## PAM SC Sub Administration for UNIX

Privileged Access Manager contains a *sub administration* feature. This lets administrators grant specific privileges that enable regular users to manage specific classes. These users are then called sub administrators.

For example, you can allow a specific user to manage users and groups only.

You can also specify a higher level of sub administration by granting access not only for specific classes, but for specified records in these classes.

## PAM SC Administration Rights for Regular Users (UNIX)

Privileged Access Manager lets you grant ordinary users (non-administrators) the rights and privileges to perform administrative tasks without being members of the Administrators group. The ability to delegate tasks by granting administrative privileges in this granular way is a significant advantage of Privileged Access Manager.

- A record in the SUDO class stores a command script to allow users to run the script with borrowed permissions.
- The data property value is the command script. This value can be modified by adding to it optional script parameter values.
- Each record in the SUDO class identifies a command for which a user can borrow permissions from another user.
- The key of the SUDO class record is the name of the SUDO record. This name is used instead of the command name when a user executes the commands in the SUDO record.

## PAM SC Program Pathing (UNIX)

*Program pathing* is an access rule associated with a file that requires that the file is accessed only through a specific program. Program pathing greatly increases the security of sensitive files. Privileged Access Manager lets you use program pathing to provide additional protection for the files in your system.

## PAM SC B1 Security Level Certification (UNIX)

Privileged Access Manager includes the following B1 Orange Book features: security levels, security categories, and security labels.

- Accessors and resources in the database can be assigned a *security level*. The security level is an integer from 1 through 255. An accessor can gain access to a resource only if the accessor has a security level equal to or greater than the security level assigned to the resource.
- Accessors and resources in the database can belong to one or more *security categories*. An accessor can access a resource only if the accessor belongs to all of the security categories assigned to the resource.
- A *security label* is a name that associates a particular security level with a set of zero or more security categories. Assigning a user to a security label gives the user both the security level and any security categories that are associated with the security label.

### NOTE

For more information about B1 Orange Book features, see the *Implementation Guide*.

## PAM SC Endpoint Management (UNIX)

Privileged Access Manager provides two ways to manage the resources in your enterprise and control who has access to them:

- **selang** - the Privileged Access Manager command language.  
The selang command language lets you make definitions in the Privileged Access Manager database. The selang command language is the command definition language.

**NOTE**

For more information about using *selang*, see the *selang Reference Guide*.

- **Privileged Access Manager Endpoint Management** - the endpoint administration interface.  
The web-based interface lets you administer remote endpoints through a central administration server.

**NOTE**

For more information about installing Privileged Access Manager Endpoint Management, see the *Implementation Guide*.

## PAM SC Safe User Substitution

The UNIX `su` command lets a user switch to another user using the password of the target user. A user who wants to switch a user ID must memorize the password of the target user, write it down, or ask the target user to use a trivial password. These actions violate several password policies. Also, the `su` command does not record who invoked the command. A user pretending to be the owner of an account is indistinguishable from the actual owner.

Privileged Access Manager includes the `sesu` utility, which is an enhanced version of the UNIX `su` command. You can configure `sesu` to prompt the user for their password as a means of authentication, rather than prompting for the password of the target user. The authorization process is based on the access rules that are defined in the SURROGATE class and, optionally, on the password of the user executing the command.

Unlike permission to `su`, permission to `sesu` does not depend on knowing the password of the target user. Instead, it depends on permissions that are specified in the database. Users remain accountable for their actions because their login identities are remembered.

If a user is a surrogate to one of the users in the `_surrogate` group, Privileged Access Manager sends a full trace of the actions of the user as the new user to the audit trail.

To protect against inadvertent use, `sesu` is marked in the file system so that no one can run it. The security administrator must mark the program as executable and `setuid` to root before you can use it.

**WARNING**

Before you use the `sesu` utility, define all users to the Privileged Access Manager database and set `sesu` prerequisites. This prevents you from opening up the entire system to users who are not defined to the product.

This page contains the following sections:

### **Set User ID Substitution Rules**

To prevent or allow users to substitute other users, set user ID substitution rules. These rules are governed through SURROGATE class resources. To define any user substitution rules, create SURROGATE records.

#### **Follow these steps:**

1. In Privileged Access Manager Endpoint Management click the Users tab, then click the Authorization and Delegation subtab.  
The Authorization and Delegation menu options appear on the left.
2. Click Users ID Substitution.
3. Click Create User ID Substitution.
4. Complete the fields in the tabbed pages, then click Save.

**Note:** For more information on SURROGATE class properties, see the *selang Reference* section.

## Set Up `sesu` for User Substitution

By default, the `sesu` utility is marked in the file system so that no one can run it. Before you make `sesu` available to your users, set database rules to ensure that it is used safely. You then lock the `su` utility so that users are forced to use the Privileged Access Manager `sesu` utility instead.

**Note:** After you complete this setup and Privileged Access Manager is running, the `su` utility does not execute. Users are forced to use the secured `sesu` utility. When Privileged Access Manager is not running, the `su` utility works.

### Set Basic User Substitution Rules

Before you start using the `sesu` utility, set up some common user substitution rules in the database. These rules prevent unknown users substituting privileged user accounts. However, these rules do permit specific users and processes to perform necessary user substitution activities.

#### Follow these steps:

1. Create a surrogate resource for the root user (USER.root) with the following attributes:

- `nobody` as owner
- Default access `none`
- All administrators have full control

This surrogate resource prevents all users from substituting root, unless explicitly authorized. All administrators are explicitly authorized to substitute root.

**Note:** You can authorize individual administrators separately or can authorize all administrators using the administrator's group.

2. Create a surrogate resource for the group of root (GROUP.other) with the following attributes:

- `nobody` as owner
- default access of `none`
- All administrators have full control

This surrogate resource prevents all users from substituting the group of root, unless explicitly authorized. All administrators are explicitly authorized to substitute the group of root.

**Note:** On most UNIX systems root's group is either `other` or `sys`.

3. Change the user substitution rules for USER.\_default as follows:

- `nobody` as owner
- Default access `none`
- Authorize root to substitute to any undefined user
- Authorize the administrators' group to substitute to any undefined user

Changing the rules prevents all users from substituting any group, unless explicitly authorized, and authorizes root and root's group to substitute any user, unless explicitly denied.

**Note:** You specifically authorize root to permit programs such as `dtlogin` to switch session ownership from root, the default X window owner (`uid=0`), to anyone else. If you do not do this, login attempts fail because Privileged Access Manager is blocking any user substitution activity that has not been explicitly authorized.

4. Change the group substitution rules for GROUP.\_default as follows:

- `nobody` as owner
- Default access `none`
- Authorize root to substitute any undefined groups
- Authorize the administrators' group to substitute to any undefined group

Changing the rules prevents all users from substituting any group, unless explicitly authorized, and authorizes root and root's group to substitute any group, unless explicitly denied.

### Example: Set Basic User Substitution Rules in `selang`

Use the following `selang` commands to set basic user substitution rules in your environment:

```
nr surrogate USER.root defacc(n) own(nobody)

auth surrogate USER.root gid(sys_admin_GID) acc(a)

nr surrogate GROUP.other defacc(n) own(nobody)

auth surrogate GROUP.other gid(sys_admin_GID) acc(a)

cr surrogate USER._default defacc(n) own(nobody)

cr surrogate GROUP._default defacc(n) own(nobody)

auth surrogate USER._default uid(root) acc(a)

auth surrogate GROUP._default uid(root) acc(a)

auth surrogate USER._default gid(sys_admin_GID) acc(a)

auth surrogate GROUP._default gid(sys_admin_GID) acc(a)
```

### ***Replace the System su Utility with the sesu Utility***

By default, the sesu utility is marked in the file system so that no one can run it. To let users substitute other users by using the sesu utility, you must enable sesu and replace the system su with this utility.

**Follow these steps: Note:** You need to be root or another authorized user to perform the following steps.

1. Permit users to run the sesu utility using the following command:

```
chmod +s /opt/CA/PAMSC/bin/sesu
```

2. Find out the location of the system's su utility using the following command:

```
which su
```

3. Rename the system's su utility using the following command:

```
mv su_dir/su su_dir/su.ORIG
```

where *su\_dir* is the directory where su resides.

4. Link the sesu utility to the su command:

```
ln -s /opt/CA/PAMSC/bin/sesu su_dir/su
```

This lets users continue to use the su command, although it now runs the sesu utility.

5. Stop Privileged Access Manager using the following command:

```
secsns -s
```

6. Modify Privileged Access Manager configuration settings using the following commands:

```
seini -s sesu.SystemSu su_dir/su.ORIG

seini -s sesu.UseInvokerPassword yes
```

The token SystemSu is set so that sesu can call the original system su utility if Privileged Access Manager is not running.

The token UseInvokerPassword is set to tell Privileged Access Manager to prompt the user for their original password instead of root's password or another user's password. The user needs to re-authenticate before the user substitution is permitted.

7. Reload Privileged Access Manager using the following command:

```
seload
```

### ***Prevent Users from Running the su Utility of the System***

Although the sesu utility is configured, anyone can run su.ORIG (the renamed system su utility) as before, with the password of root or a user. To prevent unauthorized use, use the PROGRAM class to prevent su.ORIG execution when Privileged Access Manager is running.

**Note:** If you used seuidpgm during Privileged Access Manager installation and configuration, you do not need to follow this procedure. su does not run as it has been modified (renamed to su.ORIG).

**Follow these steps:**

1. In selang, set Privileged Access Manager to monitor the renamed su utility, using the following command:

```
nr program su_dir/su.ORIG defacc(x) own(nobody)
```

2. Log in as root to change file access and modification time. Use the following command:

```
touch su_dir/su.ORIG
```

Privileged Access Manager is watching su.ORIG and, because the file has been *touched*, prevents it from being executed.

## **Define PAM SC SUDO Records**

A record in the SUDO class stores a command script so that users can run the script with borrowed permissions. The SUDO record and the sesudo command that executes the scripts control the ability to borrow permissions.

In a SUDO record, the comment property is used for a special purpose. The comment property is often known by its alternate name: the data property.

The value of the data property is the command script, with the optional addition of one or more script parameter values that are to be prohibited or permitted. The entire data property value must be enclosed in single quotes. Reference executables by their complete path names to prevent Trojan horses from taking their place.

The format for the data property is this:

```
data('cmd[;[prohibited-values][;permitted-values]] ')
```

Because the lists of prohibited and permitted values are optional, a simple data property value could be the following:

```
newres SUDO MountCd data('mount /dev/cdrom /cdr')
```

The simple value in the command means that the command sesudo MountCd executes the script mount /dev/cdrom /cdr. No particular script parameter values are prohibited; all are permitted.



Wildcards and powerful variables give you flexibility in specifying prohibited and permitted parameters. The wildcards that you can use are the standard UNIX wildcards. The following table lists the variables:

| Variable | Description                                        |
|----------|----------------------------------------------------|
| \$A      | Alphabetic value                                   |
| \$G      | ExistingPrivileged Access Manager group name       |
| \$H      | Home path pattern of the user                      |
| \$N      | Numeric value                                      |
| \$O      | User name of the Executor                          |
| \$U      | ExistingPrivileged Access Manager user name        |
| \$e      | SUDO commands with no parameters                   |
| \$f      | Existing file name                                 |
| \$g      | Existing UNIX group name                           |
| \$h      | Existing host name                                 |
| \$r      | Existing UNIX file name with UNIX read permission  |
| \$u      | Existing UNIX user name                            |
| \$w      | Existing UNIX file name with UNIX write permission |
| \$x      | Existing UNIX file name with UNIX exec permission  |

If you append a list of *prohibited* parameter values to the script:

- Separate the script from the prohibited parameter values with a semicolon, but keep them all inside the single quotes. Example: you want to prevent the user from using -9 but permit the user to use all other parameters, enter the following command:

```
newres SUDO scriptname data('cmd;-9')
```

where *cmd* represents your script.

Alternatively, define the SUDO record as follows if you do not allow any parameter values, but you want all parameters defaulted:

```
newres SUDO scriptname data('cmd;*')
```

- If a script parameter has more than one prohibited value, use the space character as a separator. Example: you want to prevent the user from using -9 and -HUP but permit the user to use all other parameters, enter the following command:

```
newres SUDO scriptname data('cmd;-9 -HUP')
```

- If more than one script parameter has prohibited values, use the pipe character (|) as a separator between sets of prohibited values. Example: you want to prevent the user from using -9 and -HUP for the first parameter of the script, and from using any existing UNIX user name for the second parameter (see the previous list of variables), enter the following command:

```
newres SUDO scriptname data('cmd;-9 -HUP | $u')
```

If the script has more parameters than you list, then your last set of prohibited parameters applies to all the remaining parameters.

If you append a list of *permitted* parameter values to the script:

- The *sesudo* utility enforces two checks: Not only must the parameter values not match any of the corresponding prohibited values; they must also match at least one of the corresponding permitted values. Separate the list of *permitted* values from the list of *prohibited* values with a semicolon, but keep them all inside the single quotes. Even if you have no list of prohibited values, you still need the semicolon; otherwise what you intend to permit is prohibited. Example: if you want to allow only the value NAME as a parameter value for the script, enter the following command:

```
newres SUDO scriptname data('cmd;;NAME')
```

As in the other list:

- If a script parameter has more than one permitted value, use the space character as a separator.
- If more than one script parameter has permitted values, use the pipe character (|) as a separator between sets of permitted values.

Example: if you have two parameters, and the first must be numeric but must not be a UNIX user name, and the second must be alphabetic but must not be a UNIX group name, enter the following command:

```
newres SUDO scriptname data('cmd; $u | $g ; $N | $A')
```

If the script has more parameters than you list, then your last set of permitted parameters applies to all the remaining parameters.

Thus, the overall format for the data property is this: first the script; then the prohibited values, parameter by parameter; then the permitted values, parameter by parameter:

```
data('cmd;
param1_prohib1 param1_prohib2 ... param1_prohibN | \
param2_prohib1 param2_prohib2 ... param2_prohibN | \
...
paramN_prohib1 paramN_prohib2 ... paramN_prohibN ; \
param1_permit1 param1_permit2 ... param1_permitN | \
param2_permit1 param2_permit2 ... param2_permitN |
...
paramN_permit1 paramN_permit2 ... paramN_permitN')
```

## PAM SC Tools for Preventing Password Attacks

The most common type of unauthorized access is that of hackers who guess passwords. Privileged Access Manager provides two tools that detect and protect against password attacks:

- serevu
- pam\_seos

Another method of protecting against password attacks is controlling passwords that are used in your environment by setting password policy rules.

### **serevu**

The serevu daemon locks the accounts of users who performed more than a specified number of login attempts. This prevents potential password attacks by rejecting further attempts to enter the account; it also prevents “dictionary attacks”.

Typically, the danger in using the user lockout utility is that it opens the system to denial of service attacks. One common type of denial of service attack is an attempt to break into the system administrator account. After a few attempts, the system administrator account is revoked and the system administrator can no longer log in. If similar attacks are performed on all critical user accounts, the system may be rendered unusable, with no way of recovering. To prevent this, the serevu daemon provides the following two modes of operation:

- The account is revoked for a specified time frame, after which it is automatically restored.
- The account is permanently revoked.

serevu does not revoke root, so the system is never locked out.

**Note:** Take special care regarding the root user password to prevent successful dictionary attacks on root.

## **pam\_seos**

pam\_seos is a Pluggable Authentication Module (PAM) that Privileged Access Manager uses for advanced account management functions. Privileged Access Manager calls pam\_seos during the login procedure of any login program. The module is a shared object that can be dynamically loaded to provide the necessary functionality upon demand.

You can configure pam\_seos to perform three actions:

- **Detect login failures**

The Account Management Component detects any failed login attempt and logs it to both the audit file and a special failed logins file. This module detects UNIX failures, not cases in which Privileged Access Manager denies access. Privileged Access Manager writes the failed login attempts to a special file. The serevu utility reads this file and uses the information to determine if and when user access should be revoked.

- **Provides debug mode**

When Privileged Access Manager denies a login, it usually does not show the reason for denial during the login session. If the pam\_seos module debug mode is set, Privileged Access Manager gives a short description of the reason for login denial. For example, "grace logins" means that the user has no remaining logins.

- **Checks for expired passwords and grace logins**

The Password Management Component invokes the segrace utility, which checks for a user password expiration and the number of grace logins. If a user password expires, and the user has no grace logins left, segrace invokes the sepass utility to allow the user to change the password.

**Note:**

- Privileged Access Manager invokes segrace only when a password change is needed.
- To obtain failed login events from SSH, the SSH version you are using must be compiled and configured to support PAM. If your version of SSH does not use PAM, Privileged Access Manager cannot detect whether a user has violated the failed login rules.

The installation program adds the relevant lines to the pam.conf configuration file, and stores the old configuration file as /etc/pam.conf.bak.

Configuration of the pam\_seos modules is performed through the seos.ini file. Set the following tokens, which are located in the [pam\_seos] section, according to the required functionality:

To use the Password Expiration and Grace Logins check, set the following token in the seos.ini file:

```
call_segrace = Yes
```

To use Login Debug Mode, set the following token in the seos.ini file:

```
debug_mode_for_user = Yes
```

To make serevu use pam\_seos login failure detection, set the following token in the seos.ini file:

```
serevu_use_pam_seos = Yes
```

## **Restrictions and Limitations**

The protection techniques that are described in this section have the following restrictions and limitations:

- On Sun Solaris, after five failed login attempts, serevu is notified.
- The pam\_seos module is only implemented in the versions of Sun Solaris, HP-UX, and Linux that support PAM.
- Enable PAM on AIX (5.3 and above) before you install Privileged Access Manager.

## **PAM SC Restrictions and Limitations**

The protection techniques that are described in this section have the following restrictions and limitations:

- On Sun Solaris, after five failed login attempts, serevu is notified.
- The pam\_seos module is only implemented in the versions of Sun Solaris, HP-UX, and Linux that support PAM.
- Enable PAM on AIX (5.3 and above) before you install Privileged Access Manager.

## PAM SC Enhanced Access Restrictions for UNIX Files and Directories

Privileged Access Manager leaves the UNIX system of permissions intact but adds a layer of enhanced access control to it.

Privileged Access Manager intercepts each of the following file access operations. The product verifies that the user has authorization for the specific operation before returning control to UNIX. The access type is in parentheses.

- File create (create)
- File open for read (read)
  - Note:** Read privileges can control whether users can perform operations that obtain information about the file (such as ls -l). Set the STAT\_intercept configuration setting to 1 to do this. For more information, see the *Reference* section.
- File open for write (write)
- File execute (execute)
- File delete (delete)
- File rename (delete, rename)
- Change permission bits (chmod)
- Change owner (chown)
- Change timestamp for example, as a result of executing the touch command (utime)
- Edit native ACL using the acledit command for systems that support ACLs (sec)
- Change directory (chdir)

Privileged Access Manager access checking differs from the native UNIX authorization in the following ways:

- Privileged Access Manager bases its authorization checks on the original user ID of the user who logged in, not on the effective user ID (euid). Example: if *user* invokes the su command to surrogate to another user, *userA* still only has access to those files to which *userA* is permitted. Surrogating to another user does *not* automatically give the original user access to the files of the target user as it does in UNIX.
- Privileged Access Manager does not give the superuser (root) automatic access to every file on the system. The superuser is subject to authorization checking like all other users of the system.
- Authorization checking is based on the following conditions: Privileged Access Manager normal and conditional access lists, day and time restrictions, security levels, security categories, and security labels.
- If you do not specifically authorize a user to access a file, Privileged Access Manager checks whether that user belongs to any group authorized to access the file.
- Each file access is audited through the normal Privileged Access Manager audit procedures.
- When deleting a file, Privileged Access Manager requires the user to have DELETE access authority to the specified file. UNIX requires the user to have WRITE authority for the parent directory.
- To rename a file, the user must have DELETE access authority to the source file and RENAME access authority to the target file. UNIX also requires that they user have WRITE access authority for the parent directory.
- All users are given permanent READ access (as a minimum) to the files /etc/passwd and /etc/group, regardless of the default setting of these files. This access prevents the system from hanging.
- The owner of a FILE object in the Privileged Access Manager database always has full access to the file protected by the object.
- The chdir access type controls the chdir command specifically, and does not execute, as UNIX does.

The following conditions are the limits of the File Protection System:

- Concerning users who are not members of the special \_restricted group, Privileged Access Manager protects only those files and directories that:

- Are defined by their individual names in the database
- Match a name pattern (for example, /etc/\*) that is defined in the database

For users that belong to the group `_restricted`, all system files are protected by Privileged Access Manager. For files that are not defined in the database, authorization is based on the `_default` record of the FILE class.

- Privileged Access Manager maintains a table of all file names and directory names (including patterns using wildcards) that indicate resources that need protection. The amount of memory available for this table is limited. Typically, the maximum number of files and directories you can define by individual names in the database is 4096. The maximum number of name patterns is 512.
- Some files receive protection even if no explicit access rules exist for them. These files include the Privileged Access Manager database files, audit logs, and configuration files.

**Note:** For more information, see the FILE class in the *Reference* section.

Privileged Access Manager supports the following access types for files.

- ALL
- CHDIR
- CHMOD
- CHOWN
- CONTROL
- CREATE
- DELETE
- EXECUTE
- NONE
- READ
- RENAME
- SEC
- UPDATE
- UTIME
- WRITE

The File Protection System is useful for protecting selected sets of files that contain sensitive data. For example, you can use Privileged Access Manager to protect the following files:

- /etc/passwd
- /etc/group
- /etc/hosts
- /etc/shadow

Use Privileged Access Manager to protect databases and all other sensitive files at your site. Grant access only to the server daemon.

Rules govern some files that always need access control even without you specifying them.

This page contains the following sections:

### **How File Protection Works**

When the `seosd` daemon starts, it performs the UNIX `stat` command for each discrete file object that is defined in the database. The daemon then builds a table in memory that contains an entry for each file object. In addition, the table contains the inode and device of the file for each discrete file. With this information, Privileged Access Manager can also protect the hard links to the files because the protection is according to device and inode. The database does not keep information about the inode and device of a file.

When you create a file rule through Privileged Access Manager:

- If the file exists in UNIX, Privileged Access Manager first performs a stat command for the file. Then it adds an entry to the file table with the inode and device information of the file.
- If the file does not exist in UNIX, Privileged Access Manager adds an entry of the name of the file to the file table (without inode and device information). This entry is the same as the entry for a generic file object. Simultaneously, the kernel keeps an indication in its internal tables that this file must be checked during creation for inode and device information. When the file is created, the kernel intercepts its creation. The kernel informs seosd of the inode of the file and device information. The seosd daemon can then update the entry of the file in the file table.

When you delete a file, Privileged Access Manager deletes its entry in the seosd file table. The entry remains in the Privileged Access Manager database in case you create it again.

## Protect Files

To define a protected file in selang, enter the following command:

```
newres FILE filename
```

For example, to register a file named /tmp/binary.bkup, enter the following command:

```
newres FILE /tmp/binary.bkup
```

**Note:** When you define a file rule without specifying its access type, the default access of NONE is assigned. In this case, the owner of the file is the only one who can access the file.

Most protected files should be protected from access by the superuser. Otherwise, any user who knows the password of the superuser gains automatic access to the files. At the same time, you can prevent all other users except the owner of the file from accessing the file.

To protect several similarly named files, use a file name pattern that includes a wildcard. The wildcards are \* (which indicates zero or more characters) and ? (which indicates any one character, other than /).

The pattern that you specify is matched against the full path name of the file so that the pattern /tmp/x\* matches files that are named /tmp/x1, /tmp/xxx, and even /tmp/xdir/a.

Patterns that Privileged Access Manager does *not* let you specify are: /\*, /tmp/\*, and /etc/\*.

### WARNING

Because file name patterns are such a powerful tool, do not experiment freely with them.

Example: The following command defines as protected every file in the /tmp directory that has a name starting with a, and ending with b. This would include a file like /tmp/xyz/xyzab :

```
newres FILE /tmp/a*b
```

## Wildcards in FILE Resource Names

By using wildcards in a file resource name, you can create a file record that corresponds to multiple files: any file with a name that matches the wildcard pattern is protected by the access authorities associated with the record.

The wildcards that you can use are:

- \* for any number of any characters
- ? for any one character

If a physical resource name matches more than one resource record name, the longest nonwildcard match is used for that resource.

Privileged Access Manager does *not* accept the following patterns in names of FILE resources:

- \*
- /\*
- /tmp/\*
- /etc/\*

### Example: Use of Wildcards in a FILE Resource

The FILE resource `/usr/lpp/bin/*` protects all files and subdirectories under `/usr/lpp/bin` (however deeply nested).

## How PAM SC File Protection Works

When the `seosd` daemon starts, it performs the UNIX `stat` command for each discrete file object that is defined in the database. The daemon then builds a table in memory that contains an entry for each file object. In addition, the table contains the inode and device of the file for each discrete file. With this information, Privileged Access Manager can also protect the hard links to the files because the protection is according to device and inode. The database does not keep information about the inode and device of a file.

When you create a file rule through Privileged Access Manager:

- If the file exists in UNIX, Privileged Access Manager first performs a `stat` command for the file. Then it adds an entry to the file table with the inode and device information of the file.
- If the file does not exist in UNIX, Privileged Access Manager adds an entry of the name of the file to the file table (without inode and device information). This entry is the same as the entry for a generic file object. Simultaneously, the kernel keeps an indication in its internal tables that this file must be checked during creation for inode and device information. When the file is created, the kernel intercepts its creation. The kernel informs `seosd` of the inode of the file and device information. The `seosd` daemon can then update the entry of the file in the file table.

When you delete a file, Privileged Access Manager deletes its entry in the `seosd` file table. The entry remains in the Privileged Access Manager database in case you create it again.

## Protect Files Using the PAM SC `selang` Command Shell

To define a protected file in `selang`, enter the following command:

```
newres FILE filename
```

For example, to register a file named `/tmp/binary.bkup`, enter the following command:

```
newres FILE /tmp/binary.bkup
```

### NOTE

When you define a file rule without specifying its access type, the default access of `NONE` is assigned. In this case, the owner of the file is the only one who can access the file.

Most protected files should be protected from access by the superuser. Otherwise, any user who knows the password of the superuser gains automatic access to the files. At the same time, you can prevent all other users except the owner of the file from accessing the file.

To protect several similarly named files, use a file name pattern that includes a wildcard. The wildcards are `*` (which indicates zero or more characters) and `?` (which indicates any one character, other than `/`).

The pattern that you specify is matched against the full path name of the file so that the pattern `/tmp/x*` matches files that are named `/tmp/x1`, `/tmp/xxx`, and even `/tmp/xdir/a`.

Patterns that Privileged Access Manager does *not* let you specify are: `/*`, `/tmp/*`, and `/etc/*`.

### WARNING

Because file name patterns are such a powerful tool, do not experiment freely with them.

Example: The following command defines as protected every file in the /tmp directory that has a name starting with a, and ending with b. This would include a file like /tmp/xyz/xyzab :

```
newres FILE /tmp/a*b
```

## Wildcards in FILE Resource Names

By using wildcards in a file resource name, you can create a file record that corresponds to multiple files: any file with a name that matches the wildcard pattern is protected by the access authorities associated with the record.

The wildcards that you can use are:

- \* for any number of any characters
- ? for any one character

If a physical resource name matches more than one resource record name, the longest nonwildcard match is used for that resource.

Privileged Access Manager does *not* accept the following patterns in names of FILE resources:

- \*
- /\*
- /tmp/\*
- /etc/\*

### Example: Use of Wildcards in a FILE Resource

The FILE resource /usr/lpp/bin/\* protects all files and subdirectories under /usr/lpp/bin (however deeply nested).

## Restrict File Access

To restrict a file from access by the superuser in selang, use a longer version of the newres command. Example: To prevent the super user from accessing the file /tmp/binary.bkup, and any other user except the user myuser, use the following selang command:

```
newres FILE /tmp/binary.bkup owner(myuser) defaccess(N)
```

This command does the following:

1. Defines /tmp/binary.bkup as a protected file.
2. Sets the user myuser as the owner of the file, granting myuser access to the file.
3. Sets the default access of the file to NONE, preventing any other user from accessing the file. To permit other users access to the file, you must explicitly define access rules for that file.

### WARNING

If you invoke the selang command under root authority and then define FILE records without explicitly specifying another user as their owner, root becomes the owner of those files. As the owner, root (or any user who logs in as root) has complete and free access to the files.

### NOTE

You can set the token use\_unix\_file\_owner in the seos.ini file to yes. This permits regular UNIX users to define access rules for the files they own.

## Prevent File Access

Sometimes it is convenient to define a FILE record that has no owner. To define a FILE record that does not have an owner in selang, use the special owner nobody.



Example: To define the file `/tmp/binary.bkup` as a protected file and prevent all users from accessing the file, enter the following selang command:

```
newres FILE /tmp/binary.bkup owner(nobody) defaccess(N)
```

This newres command ensures that even the user who defined the command, whether root or otherwise, cannot access the file. After preventing all users from accessing a file, grant one or more users access to that file explicitly.

To permit a user to access to a protected file explicitly, use the authorize command. Example: To grant the user `userJo` update access to all files in the `/tmp` directory beginning with `Jo`, enter the selang command:

```
authorize FILE /tmp/Jo* uid(userJo) acc(Update)
```

#### NOTE

Privileged Access Manager protects only those files defined in its database.

### Restrict Users from Getting File Information

If you do not provide users with *read* access permissions to a file or directory, they can still use the `stat` function to get information about the file by default. For example, a user without *read* access permissions to file `/tmp/abc` can perform the following operation:

```
ls -l /tmp/abc
```

To prevent users who do not have *read* access permissions from getting file information, set the [STAT\\_intercept](#) configuration setting to 1.

### View Default Access Authority

To view the default access of users in the `_restricted` group (when no matching records are found), use the selang `showres` command with the `_default` record of the class.

For example, to view the default access that users in the `_restricted` group have for files that are not in the Privileged Access Manager database, use the `showres` selang command to display the `_default` resource of `FILE` class:

```
showres FILE _default
```

#### NOTE

All other users have the access defined by specific Privileged Access Manager database rules.

### Use Conditional Access Control Lists

You can make access to a file conditional on the program that is used to access the file. Making file access conditional in this way is named program pathing.

#### NOTE

If the program specified to access the file is a shell script, the shell script must have `#!/bin/sh` as its first line. Because the shell script treats `#!/bin/sh` line as a comment and does not process it, do not execute the shell script following `# /home/test/test.sh` or `# sh /home/test/test.sh`.

Example: This code allows any process to update the file `/etc/passwd` under the control of the password change program `/bin/passwd`. All access attempts to the `/etc/passwd` file that do not originate from `/bin/passwd` are blocked.

```
newres FILE /etc/passwd owner(nobody) defaccess(R)
authorize FILE /etc/passwd gid(users) access(U) via(pgm(/bin/passwd))
```

The newres command defines the file `/etc/passwd` to Privileged Access Manager. This command allows any user, including the owner of the file, to read the file. The authorize command allows all users to access the file when the access is made under the program `/bin/passwd`. Once the password file is protected in this manner, any Trojan horse that inserts

entries into the `/etc/passwd` file or any update to the password file by a user of the group `users` is blocked if the user is not using the `/bin/passwd` program.

Conditional access lists are also useful for controlling access to the files of a database management system (DBMS). Usually, you permit users to access such files only through the programs and utilities supplied by the database vendor. Consider the following commands:

```
authorize FILE /usr/dbms/xyz uid(*) via (pgm(/usr/dbms/bin/pgm1)) access (U)
authorize FILE /usr/dbms/xyz uid(*) via (pgm(/usr/dbms/bin/pgm2)) access (U)
```

This set of `authorize` commands allows all Privileged Access Manager users to access the file `xyz` of the DBMS system provided the access is made by either program `pgm1` or program `pgm2`, which belong to the DBMS binaries directory. Note the use of the asterisk in the user operand. The asterisk specifies all users who are defined to Privileged Access Manager. The use of the asterisk is similar in concept to the default access. However, default access also applies to users who are not defined to Privileged Access Manager. You can use the `_undefined` group for users who are not defined in the Privileged Access Manager database.

### Use Negative Access Control Lists

You can deny a user or group specific access types using a Negative Access Control List (NACL).

With the Privileged Access Manager language (selang), use the following command to deny access:

```
auth className resourceName [gid(group-name...)] \
[uid({user-name...|*})] [deniedaccess(accessvalue)]
```

### Block Trojan Horses with the `_abspath` Group

Any relative path names in the `$PATH` variable, particularly the dot (`.`) path name meaning current directory, are a security weakness. Consider the following scenario:

- At the top of the `PATH` variable for root is the current (`.`) directory.
- A malicious user creates a destructive program—a Trojan horse—and stores it as `/tmp/lis`.
- In time, as the malicious user expects, root issues the `lis` command in the `/tmp` directory. Instead of running the usual `lis` command, root actually runs—with full administrative privileges—the Trojan horse that had been stored in the `/tmp` directory.

To eliminate this security weakness, Privileged Access Manager provides a user group named `_abspath`. All members of the `_abspath` group are forbidden to use relative path names in invoking programs.

You can add a user to the `_abspath` group as you add one to any other group. Effective at the next login, the user is forbidden to use relative path names when accessing programs.

### PAM SC Synchronization with Native UNIX Security

Although Privileged Access Manager permissions are more complex than native UNIX permissions, you can synchronize your native UNIX permissions to the product permissions. That is, you can make the permissions coincide. However, the synchronization is subject to some limitations:

- Synchronization is not retroactive. Once it is in effect, it governs all newly issued Privileged Access Manager authorization commands, but it does not govern pre-existing access rules.
- Permissions that you grant in Privileged Access Manager can be passed to UNIX. However, permissions that you grant in UNIX are not passed to Privileged Access Manager.
- Because of limitations in its own system of permissions, UNIX can be unable to adopt more than a simplified form of the Privileged Access Manager permissions. Even UNIX versions that feature access control lists (ACLs) can be unable to reflect all the complexity of the Privileged Access Manager ACLs.

UNIX platforms with ACLs that can be synchronized to Privileged Access Manager are Sun Solaris and Tru64.

Without such ACLs, you can still synchronize the traditional UNIX rwx permissions to the Privileged Access Manager permissions, to the extent possible.

The combination of the UNIX option of the authorize command and the SyncUnixFilePerms token of the seos.ini file control synchronization:

- By including the UNIX option, the authorize command calls for implementation in UNIX and in Privileged Access Manager. The command can even grant UNIX permission where permission did not exist before. When the UNIX option is *not* used, selang commands do not effect on UNIX security. Moreover, where UNIX retains a prohibition, a Privileged Access Manager permission is not effective. So the only way that selang can overcome a UNIX prohibition is with the UNIX option of the authorize command.
- In the authorize command, the UNIX option works only when the SyncUnixFilePerms token is appropriately set in the [seos] section of the seos.ini file. The token has several permitted values:
  - **no** - specifies not to synchronize ACL permissions. This value is the default.
  - **warn** - specifies not to synchronize ACL permissions, but to issue a warning if the product permissions and native UNIX permissions conflict.
  - **traditional** - specifies to adjust the rwx permissions for the group according to the Privileged Access Manager ACL (and permissions for individual users are not copied to UNIX).
  - **acl** - specifies to adjust the UNIX ACL according to the Privileged Access Manager ACL.
  - **force** - specifies to adjust the UNIX world access attribute according to the Privileged Access Manager defaccess permissions.

Any change in the SyncUnixFilePerms token value takes effect only after you restart the seosd daemon.

**Use the table of contents to access the topics in this section.**

## Example Synchronization

The following example involves a file that is named /var/temp/newdata and a user who is named fowler. The example assumes that a record in the FILE class already represents the file.

1. Shut down the seosd daemon, so you can edit the seos.ini file:

```
# secons -s
```

2. Logged in as a user with permission to edit the seos.ini file, edit the seos.ini file to make the SyncUnixFilePerms line, in the [seos] section, look like this:

```
SyncUnixFilePerms = acl
```

Remember, acl means that the UNIX option adjusts the UNIX ACL according to the Privileged Access Manager ACL. The UNIX option has this function as long as the token remains set to acl.

3. Restart the seosd daemon:

```
# seosd
```

4. Invoke selang, then issue the following selang command:

```
authorize FILE /var/tmp/newdata uid(fowler) access(r w) unix
```

The command gives fowler Read and Write access to the new data file. By specifying the UNIX option, it grants the corresponding native UNIX permissions.

## Sun Solaris Limitations

Under Sun Solaris, native UNIX ACLs are not implemented in the /tmp directory.

## Monitor Sensitive Files

The Watchdog protects the binaries of your setuid/setgid programs, and any other files you specify. The [seoswd utility](#) (the Watchdog daemon) continually checks two issues:

- Whether the [seosd daemon](#) is alive and responding. If necessary, the watchdog daemon restarts the seosd daemon.
- Whether a user has modified any trusted programs or files. If so, seoswd prevents these files from executing.

When the seosd daemon forks, it automatically executes the seoswd program to start the Watchdog.

The [seos.ini](#) file contains several tokens that control the scanning and time-out values of the watchdog. The file also contains the most up-to-date documentation on these values.

You can use the Watchdog to perform the same background checks as those checks made for the setuid and setgid programs on ordinary files. These checks include generating audit records when these files are altered.

For example, consider a configuration where only the security administrator is allowed to modify the file `/etc/inittab`. To make Privileged Access Manager monitor the file and generate an alert in any case of modification, use the following command in `selang`:

```
newres SECFILE /etc/inittab
```

The file `/etc/inittab` is now constantly monitored for modifications.

## Protect the Internal Files (UNIX)

During installation, Privileged Access Manager writes rules to protect two types of internal files:

- **Internal File Rules:** Protect configuration files, log files, and database files.  
You cannot delete internal rules.
- **Default File Rules:** Protect sensitive files such as root and server certificates that you use to encrypt and authenticate communication.  
You can delete default rules after installation.

### Internal File Rules

Internal file rules protect configuration files, log files, and database files. Internal file rules are not visible in `selang` and cannot be deleted.

Files that Privileged Access Manager protects with internal file rules have the following access rights:

- Full access for Privileged Access Manager internal processes
- Read and execute (where relevant) access for all other accessors

You can write FILE rules to replace the internal file rules. If you delete these FILE rules, Privileged Access Manager reverts to the internal file rules.

Privileged Access Manager protects the following files with internal file rules. The second column of the table lists the configuration setting that specifies the file location, where applicable.

**Note:** Some file locations are defined internally and do not have a corresponding configuration setting. You cannot configure the location of these files.

| File                  | Configuration Setting and Section in <code>seos.ini</code> | Default File Location      |
|-----------------------|------------------------------------------------------------|----------------------------|
| All database files    | [seosd] dbdir                                              | <i>ACInstallDir/seosdb</i> |
| <code>seos.ini</code> | -                                                          | <i>ACInstallDir</i>        |

|                                     |                       |                                                         |
|-------------------------------------|-----------------------|---------------------------------------------------------|
| privpgms.ini                        | -                     | <i>ACInstallDir/etc</i>                                 |
| loginpgms.ini                       | -                     | <i>ACInstallDir/etc</i>                                 |
| xdmpgms.init                        | -                     | <i>ACInstallDir/etc</i>                                 |
| nfsdevs.init                        | [seosd] nfs_devices   | <i>ACInstallDir/etc</i>                                 |
| osver                               | -                     | <i>ACInstallDir/etc</i>                                 |
| accommon.ini                        | -                     | <i>ACSharedDir</i>                                      |
| seos.audit                          | [logmgr] audit_log    | <i>ACInstallDir/log</i>                                 |
| seos.audit.bak*                     | [logmgr] audit_back   | <i>ACInstallDir/log</i>                                 |
| seos.error                          | [logmgr] error_log    | <i>ACInstallDir/log</i>                                 |
| kbl.audit                           | [kblaudit] audit_log  | <i>ACInstallDir/log</i>                                 |
| kbl.audit.bak                       | [kblaudit] audit_back | <i>ACInstallDir/log</i>                                 |
| kbl.error                           | [kblaudit] error_log  | <i>ACInstallDir/log</i>                                 |
| All files<br>(If protect_bin is ON) | -                     | <i>ACInstallDir/bin</i>                                 |
| AC                                  | [kblaudit] cmd_log    | /etc<br>Symbolic link to <i>ACInstallDir/bin/cmdlog</i> |

## Default File Rules

Privileged Access Manager creates default file rules during installation to protect sensitive files. Default file rules are visible in selang and can be deleted.

The following table lists the sensitive files that Privileged Access Manager protects with default file rules, and the access rights and permitted accessors for the files.

In the table, *PMDBDir* is the directory in which the policy model databases (PMDBs) reside, and *pmd\_name* is the name of each policy model. By default, *PMDBDir* is located at *ACInstallDir/policies*. The location of *PMDBDir* is defined in the *\_pmd\_directory\_* token in the pmd section of the seos.ini file.

| File                                          | Default Access                                 | Permitted Accessors |
|-----------------------------------------------|------------------------------------------------|---------------------|
| <i>ACInstallDir/data/crypto/crypto.dat</i>    | None                                           | sechkey             |
| <i>ACInstallDir/data/crypto/def_root.pem*</i> | None                                           | sechkey             |
| <i>ACInstallDir/data/crypto/sub.key</i>       | None                                           | sechkey             |
| <i>ACInstallDir/data/crypto/sub.pem</i>       | None                                           | sechkey             |
| <i>ACInstallDir/log/policyfetcher.log</i>     | Read                                           | +policyfetcher      |
| <i>ACInstallDir/ladb/*db.la*</i>              | Read                                           | sebuildla           |
| /etc/passwd                                   | All                                            | All                 |
| /etc/shadow                                   | All                                            | All                 |
| <i>PMDBDir/pmd_name/hsock</i>                 | Read, Write, Execute, Cre, Chown, Chmod, Utime | seagent, sepmdd     |
| <i>PMDBDir/pmd_name/pmd.ini</i>               | Read                                           | seagent, sepmdd     |
| <i>PMDBDir/pmd_name/seos_*</i>                | Read, Write, Execute, Cre, Chown, Chmod, Utime | seagent, sepmdd     |

|                                |                                                |                 |
|--------------------------------|------------------------------------------------|-----------------|
| <i>PMDBDir/pmd_name/socket</i> | Read, Write, Execute, Cre, Chown, Chmod, Utime | seagent, sepmdd |
|--------------------------------|------------------------------------------------|-----------------|

## Protect setuid and setgid Programs

Set user ID (setuid) programs are among the most frequently used programs at a UNIX site. A process that invokes a setuid program automatically acquires the identity of the owner of the setuid program. If the owner of a setuid program is root, then any user automatically becomes a superuser by invoking the setuid program. When the setuid program starts, the process performs any task which a superuser has permission for. Ensure that the setuid programs perform only the required task. Back doors or shells within a setuid program grant the user access to everything on the system.

Privileged Access Manager uses the PROGRAM class to protect setuid and setgid programs. Upon installation, Privileged Access Manager permits any program execution by default. After you define trusted programs in the database, you can change the behavior of Privileged Access Manager so that execution of a setuid or setgid program is prohibited unless the program is defined as a trusted program. Example: to allow /bin/ps (the process status program) to run as a setgid program (as it is supposed to), use the following selang command:

```
newres PROGRAM /bin/ps defaccess(EXEC)
```

Privileged Access Manager registers the program /bin/ps as a trusted program. The product then calculates and stores the following information about the program: the CRC, inode number, size, device number, owner, group, permission bits, last modification time, and, optionally, other digital signatures in a record in the PROGRAM class of the database.

The Watchdog periodically checks the CRC, size, inode, and the rest of the characteristics of the program. If any of these values have changed, the Watchdog automatically asks seosd to remove the program from the trusted programs list and deny access to it. This ensures that no one can misuse the program by modifying or moving setuid programs. The permission in the example newres command allows all users, including those not defined in the database, to run the /bin/ps command.

Untrusted setuid programs are possibly the most dangerous security loophole of UNIX-based operating systems. By using the trusted access rules of the program, the security administrator can restrict the use of setuid to certain trusted programs that were tested and checked to ensure their integrity. However, any user cannot automatically start a trusted executable. The access rule must specify explicit users and groups that are granted access to that setuid program. Example: the following set of selang commands grants the execution of /bin/su only to the System Department users (group sysdept):

```
newres PROGRAM /bin/su defaccess(NONE)
authorize PROGRAM /bin/su gid(sysdept) access (EXEC)
```

Use an asterisk (\*) to specify all users who are defined in the database. For example, to permit all users who are defined to Privileged Access Manager to perform the su command, enter the following command:

```
authorize PROGRAM /bin/su uid(*) access (EXEC)
```

This description is also true for setgid executables.

You can use the nr and er commands to register the setuid and setgid programs in the PROGRAM class. Important non setuid and setgid programs can be registered in the PROGRAM class similarly. Define a FILE rule for these programs to prevent unauthorized users from upgrading them. If you want to allow the program execution when it is untrusted (after upgrade, the program is executed without being retrusted), set the blockrun property to no.

- If the blockrun property is set to yes, the program is not executed until it is retrusted and is not allowed to access any file that the relevant PACL would allow. The PACL is effectively disabled until the program is retrusted.
- If the blockrun property is set to no, the program is executed. However, the program cannot access any resources the relevant PACL would allow.

To set the value of the blockrun property to yes, use the following editres/newres command:

```
er program /bin/p blockrun
```

To set the value of the blockrun property to no, use the following editres/newres command:

```
er program /bin/p blockrun-
```

By default, for all the programs that are registered in the PROGRAM class, the blockrun property is set to yes. You can change this using the SetBlockRun token in the seos.ini file. Refer to the seos.ini file description for details.

#### NOTE

Privileged Access Manager uses the PROGRAM class and not the FILE class to protect setuid and setgid programs.

## Kernel Modules Load and Unload Protection

A *kernel module* is a component of the UNIX operating system that you can load to extend the running kernel. You can unload it when it is no longer required. The kernel module adds flexibility, letting you load functionality as required. You avoid wasting memory resources that would otherwise be required to cover all possible expected functionality in the base kernel.

You can disable and enable kernel module protection in Privileged Access Manager. If you enable kernel module protection, Privileged Access Manager intercepts the system calls that load and unload a kernel module. The product then checks the requested access against the associated record in the database, which is a record of class KMODULE. When access is requested for a kernel module record, the requested access is either "load" or "unload".

On all non-Linux systems, the name of the KMODULE record must match the name of the kernel module file, not the full path. This is because the name of the module is the same as the name of the file. On Linux, the name of KMODULE record must match only the name of the kernel module, which can differ from the actual file name. Changing the file name on Linux does not change the module name which Linux uses and the KMODULE record remains valid.

If you enable file path checking on kernel module loads and the requested access is load, Privileged Access Manager performs the following extra checks:

- The filepath property in the KMODULE record holds only valid absolute file paths.
- The files in the path name filepath have modules that match the KMODULE record name.
- The kernel module matches the KMODULE properties (filepath for non-Linux systems, signature for Linux systems).

#### NOTE

Privileged Access Manager produces a unique signature for the kernel module file on Linux systems, and inserts this as the value of the signature property in the kernel module record. Privileged Access Manager checks the signature on each access. You do not need to enter the signature yourself, because Privileged Access Manager calculates and inserts it automatically. However you can do so using the seretrust utility.

**Use the table of contents to access the topics in this section.**

## Protect a Kernel Module

You can protect the loading and unloading of kernel modules, and so help protect the operating system.

### To protect a kernel module:

Ensure that you have enabled kernel module protection. Create a KMODULE record in Privileged Access Manager.

1. 1. To create a kernel module, define:
  2. • The name of the kernel module

On all non-Linux systems, the name of the KMODULE record must match the name of the kernel module file (not the full path). This is because the name of the module is the same as the name of the file. On Linux, the



name of KMODULE record needs to match only the name of the kernel module, which, might be different from the actual file name.

- The owner of the record (defaults to the user creating the module)
- (Optional) The absolute file path to the kernel module file, or a list of file paths if there is more than one version of the module.

#### NOTE

On HP and Solaris systems, you can define the special kernel module `_ALL_MODULES` to protect the unloading of all kernel modules.

1. Define the users or groups that are authorized to load and unload the module.

#### Example: Protect a Kernel Module Using `selang` Commands

The following `selang` commands define and authorize a kernel module `serial.o` to Privileged Access Manager, and authorizes the enterprise user `kadmin` to load and unload it:

```
newres kmodule serial.o owner(kadmin) defaccess(none) \
filepath(/lib/modules/2.2.19/serial.o:/lib/modules/2.2.20/serial.o)
authorize kmodule serial.o access(load, unload) xuid(kadmin)
```

### Enable and Disable Kernel Module Protection

When kernel module protection is enabled, Privileged Access Manager checks the loading and unloading of the kernel modules that are defined in the database.

By default, Privileged Access Manager enables protection of kernel modules.

To enable or disable kernel mode protection, enable or disable the KMODULE class. For example, use the `setoptions` command.

#### Example: Enable Kernel Mode Protection Using `selang`

The following `selang` command enables kernel mode protection:

```
setoptions class+(kmodule)
```

#### Example: Disable Kernel Mode Protection Using `selang`

The following `selang` command disables kernel mode protection:

```
setoptions class-(KMODULE)
```

### Enable and Disable File Path Checking on Kernel Module Loads

If kernel module protection is enabled, you can also enable file path checking on kernel module loading. When this is enabled, Privileged Access Manager checks that the kernel module to be loaded matches the `filepath` property of the KMODULE record (for non-Linux systems), or matches the signature of the KMODULE record (for Linux systems).

To enable file path checking, set the `special_check` token to `yes` in the `seosd` section of the configuration file `seos.ini`. The default is `no`.

Privileged Access Manager does file path checking only if file path checking and kernel mode protection are both enabled.

#### Example: Enable File Path Checking for Kernel Module Loads Using the `seini` Utility

To enable file path checking for kernel module loads, you can use the `seini` and `secons` utilities as follows:

```
seini -s seosd.special_check yes
```



```
secons -rl
```

## Protect Binary Files from the kill Command

Protect mission-critical processes, such as database servers or application daemons, against denial of service attacks. The native UNIX security system bases its process protection on the process user ID. This implies that under native UNIX, root can do anything to any process. Privileged Access Manager adds to UNIX process protection by defining rules that are based on the executable file running in the process. Privileged Access Manager process protection is *independent* of the user ID of the process. A record in the PROCESS class must define every process that Privileged Access Manager protects.

For example, to protect the ASCII viewer /bin/more from being killed, follow this procedure:

1. Start selang.

2. Enter the following selang command:

```
newres PROCESS /bin/more defaccess(N) owner(nobody)
```

This command defines /bin/more as a process to be protected from kill attempts; therefore the default access is *none* (N). The **owner(nobody)** setting ensures that even the user who defined this rule cannot kill the /bin/more process.

3. Exit selang.

4. Test the rules that Step 2 defined:

a. Enter the command:

```
/bin/more /tmp/seosd.trace
```

b. Assuming the file /tmp/seosd.trace is large enough to keep /bin/more from exiting immediately, press Ctrl+Z to suspend the /bin/more process.

c. Try to kill the suspended job by entering the command:

```
kill %1
```

Your attempt fails, with Privileged Access Manager displaying the Permission denied message.

To make an exception that permits a specific user to kill the /bin/more processes, enter the selang command:

```
authorize PROCESS /bin/more uid(username)
```

### NOTE

Use the same procedure to protect other binary executables on your system from being killed.

Privileged Access Manager protects regular kill signals (SIGTERM) and the kill signals that an application cannot mask (SIGKILL and SIGSTOP). It passes other signals, such as SIGHUP or SIGUSR1, to the process to determine whether to ignore or react to the kill signal.

## Control Login Commands

This section provides information about control login commands.

**Use the table of contents to access the topics in this section.**

### Control the Login Process

Privileged Access Manager provides two types of login protection: by terminal, and by application. Using the TERMINAL class, you can establish which users can log in from which terminals or hosts.

### NOTE

For more information about the TERMINAL class, see the *Reference Guide*.

You can also control which user or group can log in using a certain login application such as Telnet, ftp, and rlogin with the LOGINAPPL class. By establishing the access rules of the class, you define specific rules for each login application. For instance, you can define rules that enforce the following conditions:

- Permit all users to ftp to your host
- Permit a limited number of users to Telnet to your system
- Permit no one to rlogin to the system

Each record in the LOGINAPPL class defines access rules for a specific login application.

## Examples LOGINAPPL

Example: The following procedure permits only an anonymous user to use the ftp application:

1. Change the ftp default access to none with the following selang command:

```
cr LOGINAPPL FTP defaccess(NONE) owner(nobody)
```

2. Permit the user anonymous to use ftp with the following selang command:

```
auth LOGINAPPL FTP uid(anonymous) access(X)
```

To restrict users from the group that is named account to use only telnet:

1. Block the use of rlogin and rsh with the following selang command:

```
auth LOGINAPPL(RLOGIN RSH) gid(account) access(N)
```

2. Permit the group that is named account to use telnet with the following selang command:

```
auth LOGINAPPL TELNET gid(account) acc(X)
```

### NOTE

The previous example shows RLOGIN and RSH restrictions, but other login programs should be included as well.

### NOTE

Whenever you add or use a new login program, you must add a LOGINAPPL record.

The login interception sequence always starts with setgid or setgroup events, which are called *triggers*. The sequence ends with a setuid event that changes the identity of the user to the real user who logged in.

Login applications issue various system calls, which Privileged Access Manager uses to monitor login activity. These login sequences are preset for standard login applications. You can see them by studying the Privileged Access Manager trace file.

### NOTE

For more information about the LOGINAPPL class and setting a sequence, see the *selang Reference Guide*.

## Enable SFTP Login Interception

When a user logs in to an endpoint using SFTP, the SFTP application uses SSH to authenticate the user. When Privileged Access Manager intercepts the login attempt from the SFTP application, it treats the login as an SSH login by default. The product uses the rules for the SSH LOGINAPPL record to permit or deny the login attempt.

To configure Privileged Access Manager to distinguish SFTP and SSH login attempts and to write separate rules for SFTP and SSH logins, enable SFTP login interception.

### To enable SFTP login interception

1. Open a command prompt window on the endpoint.
2. Enter the following selang command:

```
er LOGINAPPL SSH loginflags(EXECLOGIN)
```

This command specifies that the trigger for SSH logins is the first EXEC action that a process performs.

### 3. Enter the following selang command:

```
er LOGINAPPL SFTP loginpath(path) defaccess(a)
loginpath(path) Specifies the full path to the SFTP login application.
```

```
er LOGINAPPL SFTP loginpath(path) defaccess(a)
```

– loginpath(*path*)

Specifies the full path to the SFTP login application.

This command creates a LOGINAPPL record that is named SFTP. The command defines the path to the SFTP login application, and specifies that all users can use SFTP to log in to the endpoint if no additional restrictions exist.

### Example: Enable SFTP Login Interception

This example enables SFTP login interception for the SFTP login application located at /usr/libexec/openssh/sftp-server. The first selang command also specifies that Privileged Access Manager uses PAM login interception for SSH logins:

```
er LOGINAPPL SSH loginflags(EXECLOGIN, PAMLOGIN)
er LOGINAPPL SFTP loginpath(/usr/libexec/openssh/sftp-server) defaccess(a)
```

#### NOTE

For more information about the LOGINAPPL class, see the *selang Reference Guide*.

## Control Generic Login Applications

Privileged Access Manager can also control and protect generic login applications. This feature enables you to protect groups of login applications that match a certain rule with a generic pattern. To define a generic login application, use the LOGINAPPL class.

### Define a Generic Login Application

To define a generic login application with selang, use the same commands as setting regular login restrictions. The exception is the LOGINPATH parameter. This parameter must include a generic path composed of a regular expression using one or more of the following characters: [, ], \*, ?. For example, to define a generic Telnet application, issue the following command:

```
er LOGINAPPL GENERIC_TELNET loginpath(/usr/sbin/in.tel*)
```

### Generic Login Program Interception

With regular login restrictions, these rules are the activated rules:

- If a LOGINAPPL object that has the intercepted login program that is specified for the loginpath property exists in the database, the rules for that object apply.
- For generic LOGINAPPL objects, Privileged Access Manager follows these steps:
  - a. seosd searches for an exact match for the intercepted login application (a matching login path for the LOGINAPPL object). If found, the rules for that object apply.
  - b. If not found, the search continues for a LOGINAPPL object with a generic login path that matches.
  - c. If there is more than one match, the rules for the object with the more specific match apply.

## Define User Authority to Use Terminals

One of the most effective ways to block intruders from accessing the system is by terminal protection, which is the source of the login. The source can be the host or the terminal (such as an X terminal or a console) from which the user logs in.

In modern architecture, a terminal is no longer the teletype device UNIX was developed for. On most sites, a pseudo terminal is allocated through the pseudo terminal server (PTS) or by the X window manager. The name of the terminal is a meaningless symbol for the security system. Privileged Access Manager protects what we understand as a terminal. The product implements terminal protection during the login stage, when the product defines a terminal in one of three ways:

- When the user logs in from an X terminal using the XDM login window, Privileged Access Manager takes the IP address of the X terminal that is translated to host name (from /etc/hosts, NIS, or DNS) to be the terminal that is used for the login request. The product can also protect using the IP addresses if the translation to the host name fails or if you prefer to use IP addresses.
- When the user logs in from a dumb terminal, the TTY name identifies the terminal.
- When the user logs in from the network (through Telnet, rlogin, rsh, and so on), the requesting IP address that is translated to the host name (through /etc/hosts, NIS, or DNS) is taken to be the terminal name.

You can define login rules for a specific host by defining this host in the **TERMINAL** class. Add the appropriate users and groups to the access list of the object. For each login source, you can also limit the days and hours in which log in from this host or terminal is allowed. To do this, set the day and time restrictions for the **TERMINAL** object. Use wildcards in the **TERMINAL** class to define hosts that match a pattern (host name or IP address).

Usually, highly authorized users such as the superuser or system administrators are restricted to terminals that are located in secure places. Intruders and hackers who want to enter the system as superuser are not able to do it from their own remote stations. They have to work from one of the authorized terminals, which should be in a secured location.

When logging in from the network, you cannot be certain that the user is indeed sitting in front of the host console. The user could be sitting in front of any terminal that is attached to that host or communicating from any other node in the network authorized to receive services from the requesting host. Permitting a user to log in from another host implies that we permit login to that user not only from that specific station but also from any other terminal authorized by that station. To ensure isolation between departments, define terminal groups. Allow users of each department to work only from the terminal group of their department.

Unlike other resources, in terminal authorizations the more the user is authorized to access information, the lower the terminal authorization of the user should be. The superuser must be the most restricted user in terminal access. This restriction ensures that nobody can log in as root from remote unsafe terminals.

When defining terminals, Privileged Access Manager requires you to specify the owner of the terminal definition explicitly. The reason is that if the root user, as the security administrator, becomes the owner of the terminal by default, it makes the terminal eligible for superuser login. In most cases, this is not wanted. To prevent such mistakes that might unintentionally cause loopholes, Privileged Access Manager makes you define an owner when defining the terminal.

To define the terminal `tty34`, use the following command:

```
newres TERMINAL tty34 defaccess(none) owner(userA)
```

This command creates a record for the terminal `tty34`, sets its default access to `NONE`, and defines `userA` as its owner. `userA`, as the owner of the terminal, is automatically allowed to enter the system through terminal `tty34`.

To prevent all users from logging in from the terminal `tty34`, specify `nobody` as the owner:

```
newres TERMINAL tty34 defaccess(none) owner(nobody)
```

To permit a user to log in from a particular terminal, enter the following command:

```
authorize TERMINAL tty34 uid(USR1)
```

This command permits `USR1` to log in from terminal `tty34`.

Permission to use a terminal can also be granted to a group. For example, the following command permits members of the group `DEPT1` to use the terminal `tty34`:

```
authorize TERMINAL tty34 gid(DEPT1)
```

To define a group of terminals (known as a terminal group), enter the following command:

```
newres GTERMINAL TERM.DEPT1 owner(ADM1)
```

To add member terminals to the terminal group TERM.DEPT1, enter the following command:

```
chres GTERMINAL TERM.DEPT1 mem(tty34, tty35)
```

To authorize USR1 to use this terminal group, enter the following command:

```
authorize GTERMINAL TERM.DEPT1 uid(USR1)
```

This grants USR1 the authority to use both tty34 and tty35.

## Restrict Terminals for Root Users

Another issue to consider is the default rule of the TERMINAL class. At the initial implementation stages, the default is set to permit anything that is not defined. If this thing is a TERMINAL, this default could be a shortcoming.

Consider the following situation: A site has a few hundred terminals, and you want most users to be able to log in from any terminal. However, you want the root user to be able to log in only from two predefined terminals.

First, consider that setting the default of the TERMINAL class to READ enables anyone, including root, to log in from any terminal that does not have a specific TERMINAL record in the database. You do not want the superuser to be able to log in from any terminal. Also consider that setting the default of the TERMINAL class to NONE forces you to define each terminal in the database. This situation can be impractical.

To solve this problem, Privileged Access Manager supports the definition of an access control list within the \_default record of the TERMINAL class. The following commands show you how to restrict root to two terminals with minimum effort:

```
newres TERMINAL term1 defaccess(N) owner(root)
newres TERMINAL term2 defaccess(N) owner(root)
newres TERMINAL _default defaccess(R)
authorize TERMINAL _default uid(root) access(N)
```

The first two commands define term1 and term2 as terminals owned by root, so they are eligible for superuser login. The newres TERMINAL \_default and chres commands set the default access to READ, so that any terminal that is not defined in the database is accessible to anyone. The authorize command explicitly denies access of the superuser to undefined terminals.

### NOTE

The UACC class still exists; you can use it to specify the default access of a resource. However, using \_default records to specify the default access of a resource is much easier.

## Recommended Restrictions

Restrict the use of the loopback terminals, local host terminals, and station host names if the default access for the TERMINAL class is READ. Allowing users to use these terminals permits all other users to substitute their own user IDs if they know the password of the target user. For example, consider the following scenario:

- User U is allowed to work from terminal T.
- Terminal T is not allowed for superuser login.
- User U is not authorized to substitute user ID to root.
- User U managed to get the superuser password.
- All users are permitted to log in from terminal loopback.

User U can bypass this set of access rules by simply performing the command `telnet loopback`, specifying the user ID `root`, and supplying the password. Now a superuser session has started from terminal T, which is not supposed to allow superuser login. A user can similarly bypass access rules by exploiting the local host or the host name of the station.

To restrict these three vulnerabilities, use the following definitions:

```
newres TERMINAL loopback defaccess(N) owner(nobody)
newres TERMINAL localhost defaccess(N) owner(nobody)
chres TERMINAL hostname defacc(N) owner(nobody)
```

An alternative approach to preventing this security breach is to limit the TCP requests for `telnet`, `ftp`, and so forth, from local host.

Yet another option is to set default access for the `TERMINAL` group to `NONE`, then specify `TERMINAL` and `GTERMINAL` rules.

## Password Checking and Login Restrictions

Privileged Access Manager does not replace the `/bin/login` executable. Even when Privileged Access Manager is running, passwords continue to be checked against `/etc/passwd`, the shadow password file, or the NIS `passwd` map. But Privileged Access Manager also performs more checks, described in the following section.

## Defining Time and Day Login Rules

Information security is most vulnerable in times of low activity. Late hours of the night and weekends are ideal times for breaking in, because fewer people are available to monitor the audit records. Setting up appropriate terminal authority rules forces an intruder to use a terminal that is in a protected location. Setting up days-of-week (DOW) and time-of-day (TOD) access rules forces the intruder to attempt break-ins during work hours when offices are open and active. This combination severely restricts break-ins.

Limiting the days and hours in which a user can log in is done on a user-by-user basis. To define the DOW and TOD login restrictions for a user, use the following command:

```
chusr USR1 restrictions(days (Mon,Tue,Wed)time (800:1700))
```

This command permits user `USR1` to log in only between 8:00 and 17:00 on Mondays, Tuesdays, and Wednesdays. `USR1` cannot log in outside the specified time on the specified days, or on days other than those specified.

The `days` parameter also accepts the values `ANYDAY` (allow logins on all seven days of the week) and `WEEKDAYS` (allow logins Monday through Friday). The `time` parameter also accepts the value `ANYTIME` (allow logins at any time of the day).

### NOTE

You can apply the DOW and TOD restrictions to *many* resources defined in the database. This feature is useful for giving terminals and terminal groups limited periods of usability.

## Disabling Concurrent Logins

Most UNIX-based operating systems allow concurrent logins. But if a user is permitted to log in from more than one terminal, other users can log in from elsewhere and can masquerade as that user while that user is logged in.

After you log in, Privileged Access Manager allows you to disable your own concurrent login permission. Doing so ensures that no one else can log in as you from another terminal. However, you can still log in repeatedly from the particular terminal that you are using. Use the `secons` command with the following switches:

```
# secons -d- (disables concurrent login)
```

```
# secons -d+ (enables concurrent login)
```

Any user can issue the -d option. (All other options are only allowed for users with the ADMIN or OPERATOR attribute). Users who want to disable concurrent logins can use this command in their initial scripts. Although they are then able to open as many windows as they want, they cannot log in from a second terminal.

#### NOTE

If you use the secons -d- command to prevent concurrent logins, you must remember to use secons -d+ before logging out, to avoid being locked out of the system. If you forget to reinstate concurrent logins and try to log in again, Privileged Access Manager allows you to log in provided no process with the same user ID is running.

## Limit Concurrent Logins for a User

Privileged Access Manager can control the number of concurrent logins in two ways:

- **Administrator Level**

Set a systemwide definition in the database of the number of concurrent sessions a user can have. You can set this value globally, for a profile group, or for individual users.

- **User Level**

Users individually control the number of concurrent logins allowed for them. This way, when logging in, users can block the option of more login sessions with their names, thus protecting themselves.

#### NOTE

The number of concurrent logins is independent of the number of sessions the user is running on a particular terminal. Multiple sessions on one terminal are considered as a single login. The concurrent-logins limit restricts the number of *terminals* a user can concurrently log in from, not the number of logins from each terminal.

## Limit Concurrent Logins Globally

In `selang`, enter the following command:

```
setoptions maxlogins(NumLogins)
```

## Limit Concurrent Logins Individually

In `selang`, enter the following command:

```
chusr username maxlogins(NumLogins)
```

The concurrent logins limit set for a user overrides the systemwide limit. To prevent Privileged Access Manager from enforcing the concurrent logins limit for a specific user, set the concurrent logins limit to zero for the user. You cannot use `selang` if you set the maximum number of concurrent logins to one.

## Recognize a Login Event

Privileged Access Manager does not treat all attempts to change the user ID of a process as login events. Usually a program attempts to change its user ID with a `setuid` system call. The SURROGATE class controls these events, which are not necessarily considered login events. These events do not necessarily change the user identity from the point of view of Privileged Access Manager.

Privileged Access Manager always preserves the original user identity--the identity with which the user logged in initially. Ordinary `setuid` system calls do not cause Privileged Access Manager to register a change in user identity.

For Privileged Access Manager to recognize the identity change, it must recognize this event as a login event. The product recognizes login events using the following rules:

- The program that attempts to change the identity is defined as a *login program*. All programs in the LOGINAPPL class are login programs.
- The program executes a series of system calls corresponding to its definition in the LOGINAPPL class.

When you begin an administration session (in *selang* or Privileged Access Manager Endpoint Management), Privileged Access Manager performs a dummy login event. This event is not a true login; rather, Privileged Access Manager performs certain internal checks, which are similar to log in checks.

#### NOTE

For more information, see the SEQUENCE property for the LOGINAPPL class in the *selang Reference Guide*.

At the start of an administration session, the user name is checked in the machine to be administered. You get access to this machine for administration only if you have WRITE access for the terminal from which you perform the session.

For example, if you are logged in to host Minerva and would like to administer Privileged Access Manager on host Artemis, two conditions are necessary:

- A TERMINAL object called Minerva (or the relevant fully qualified name) is in the database record for Artemis.
- You are listed in the ACL of this object with WRITE permission.

These conditions are checked before any other user authority check. You also need administrative authority in the database.

## Protect TCP/IP Services

Protecting TCP/IP services is most important for file servers that contain sensitive data. These servers must provide certain services only to trusted stations, and not to intruders or computers that are unknown to the host.

## Restrict TCP IP Services

In an open network, any station can request services from other computers on the network. The TCP/IP protocol can be used to supply many services. Some of these services, such as *rlogin*, *rcp*, *rsh*, *ftp*, *telnet*, and *rexec*, are common to all UNIX-based operating systems. Others are provided by in-house and third-party software.

Privileged Access Manager intercepts the accept processes of TCP/IP at the host computer and determines whether the accept program should continue normally or be overridden. Privileged Access Manager bases its decision on access rules governing hosts and services that you define. You can create TCP/IP access rules in the database to specify the computers and networks that are allowed to receive services such as file transfers, remote login, and remote shell from a specific computer.

The following examples show how TCP/IP access rules can be defined and set to efficiently block unwanted outsiders. If you have not yet had time to develop a complete database, you may want to let any station that is not defined in the database receive any service. If so, set the HOST record in the UACC class as follows:

```
chres UACC HOST defaccess(READ)
```

A station that is to have access rules for TCP/IP services from the local host is defined in a record in the database under the HOST class. For each of these stations, the services allowed are listed in the record. For example, the following command sequence defines a record for station *ws5* and denies it from receiving any TCP/IP service from the local host:

```
newres HOST ws5
```

```
authorize HOST ws5 service(*) access(NONE)
```

The following command allows *ws5* to perform *telnet* to the local computer:



```
authorize HOST ws5 service(telnet)
```

These settings allow users to telnet to the local computer, which means that the remote user must specify a user name and password before using the local system. To allow a station to receive all TCP/IP services from the local computer, you can use an asterisk in the service keyword. For example, the following command allows ws5 to invoke any TCP/IP service from the local computer:

```
authorize HOST ws5 service(*)
```

The service can be specified in several ways, some of which involve the *port number*. The port number is an identification number for a service. All services have port numbers, and the port numbers are mapped to the services in the file `/etc/services`. You can specify a service in the following ways:

- By its name as defined in the file `/etc/services`
- By its port number
- As a range of port numbers
- As an RPC port that is listed in the `/etc/rpc` system file

For example, the following command permits ws5 to receive any TCP/IP service whose port number falls between 7045 and 7050:

```
authorize HOST ws5 service(7045-7050)
```

In many cases, it is more economical to define a group of hosts and set its permissions once, instead of making permissions for each individual computer. Privileged Access Manager provides the GHOST class, where each GHOST record defines a group of hosts. To define a GHOST record and add hosts to its member list, enter the following commands:

```
newres GHOST gh1 mem(ws2, ws3, ws5)
```

```
authorize GHOST gh1 service(ftp)
```

The `newres` command defines a group of hosts called `gh1` that contain the members `ws2`, `ws3`, and `ws5`. The `authorize` command allows all three stations to receive `ftp` (file transfer) services.

Managing host groups is easier than managing individual stations, but to supply more flexibility, Privileged Access Manager also supports the definition of network access rules. Networks are defined in the HOSTNET class. For example, consider the following set of commands:

```
newres HOSTNET hn1 mask(255.555.0.0) match(192.168.0.0)
```

```
authorize HOSTNET hn1 service(*) access(NONE)
```

```
authorize HOSTNET hn1 service(ftp)
```

- In the first line, the `newres` command, defines a network called `hn1`. With its `mask` and `match` values, it specifies that any computer with an IP address whose first two qualifiers are `192.168` is considered as coming from the `hn1` network.
- The combination of the second and third lines permits any station from the `hn1` network to perform `ftp`, but not any other service, in the host computer.

Another method that this product provides for defining TCP/IP access rules is name-pattern access rules. The product supports the definition of generic records in the HOSTNP class (host name pattern) with wildcards.

**Note:** For information on how Privileged Access Manager performs string matching, see the *Selang Reference* section.

For example, the following command sequence permits all hosts whose names start with the characters `lin` and end with the characters `.org.com` to receive all TCP/IP services on the local host:

```
newres HOSTNP lin*.org.com
authorize HOSTNP lin*.org.com service(*).
```

**Note:** Hosts that are managed by NIS must be identified by their official names that appear in a NIS map and not by their aliases. The chart in the following section summarizes the TCP/IP check flow.

## Use the TCP Class

You can specify protection by service instead of by host, by using the TCP class.

### NOTE

For more information about the TCP class, see the *Reference Guide*.

Use the TCP class to control incoming *and* outgoing services.

For example, the following commands create a record for the `ftp` service, with `READ`, meaning the service can be used, as default access type. This example also prevents hosts that match the name pattern `PUBLIC*` from receiving the service.

```
newres TCP ftp defaccess(READ)
authorize- TCP ftp hostnp(PUBLIC*) access(N)
```

You can also specify that a particular user or group be only permitted to receive a particular service. For example, to allow all users to `ftp` to a host called `hermes`, but to specify that only members of the group that is called `acctng` can access `hermes` with `Telnet`, enter the following commands:

```
newres HOST hermes
newres TCP ftp owner(nobody) defaccess(read)
newres TCP telnet owner(nobody) defaccess(read)
authorize TCP ftp uid(*) host(hermes) access(write)
authorize TCP telnet gid(acctng) host(hermes) access(write)
```

### NOTE

`defaccess(read)` disables outgoing services. `defaccess(write)` disables incoming services.

### NOTE

If the `HOST` class is active (that is, if it is used as a criterion for access), then the `TCP` class cannot effectively be active. You can use the command `setoptions class- HOST` to deactivate the `HOST` class; then use the command `setoptions class+ TCP` (if necessary) to activate the `TCP` class. Deactivating the `HOST` class automatically deactivates `GHOST`, `HOSTNET`, and `HOSTNP` as well.

Also, if the `TCP` class is active, use the `setoptions` command `class- CONNECT` to deactivate the `CONNECT` class.

## Streams Module for Network Interception

By default, the `TCP` class is not active. Before you activate the `TCP` class, the `CONNECT` class, or the `HOST` class, be sure that the streams module is enabled.

To load the Privileged Access Manager streams module on Solaris, complete the following steps:

1. Stop Privileged Access Manager. Enter the following command:

```
secons -s
```

2. Enter the following command:

```
SEOS_load -s
```

3. Start Privileged Access Manager. Enter the following command:

```
seload
```

**NOTE**

If you attempt to activate the TCP class when the streams module is not loaded, an error appears:

```
ERROR: className class cannot be activated when streams are not loaded.
```

```
Please use SEOS_load -s to load the streams.
```

The algorithm for incoming authorizations is:

Figure 39: File\_Incoming\_Authorization\_Algorithm

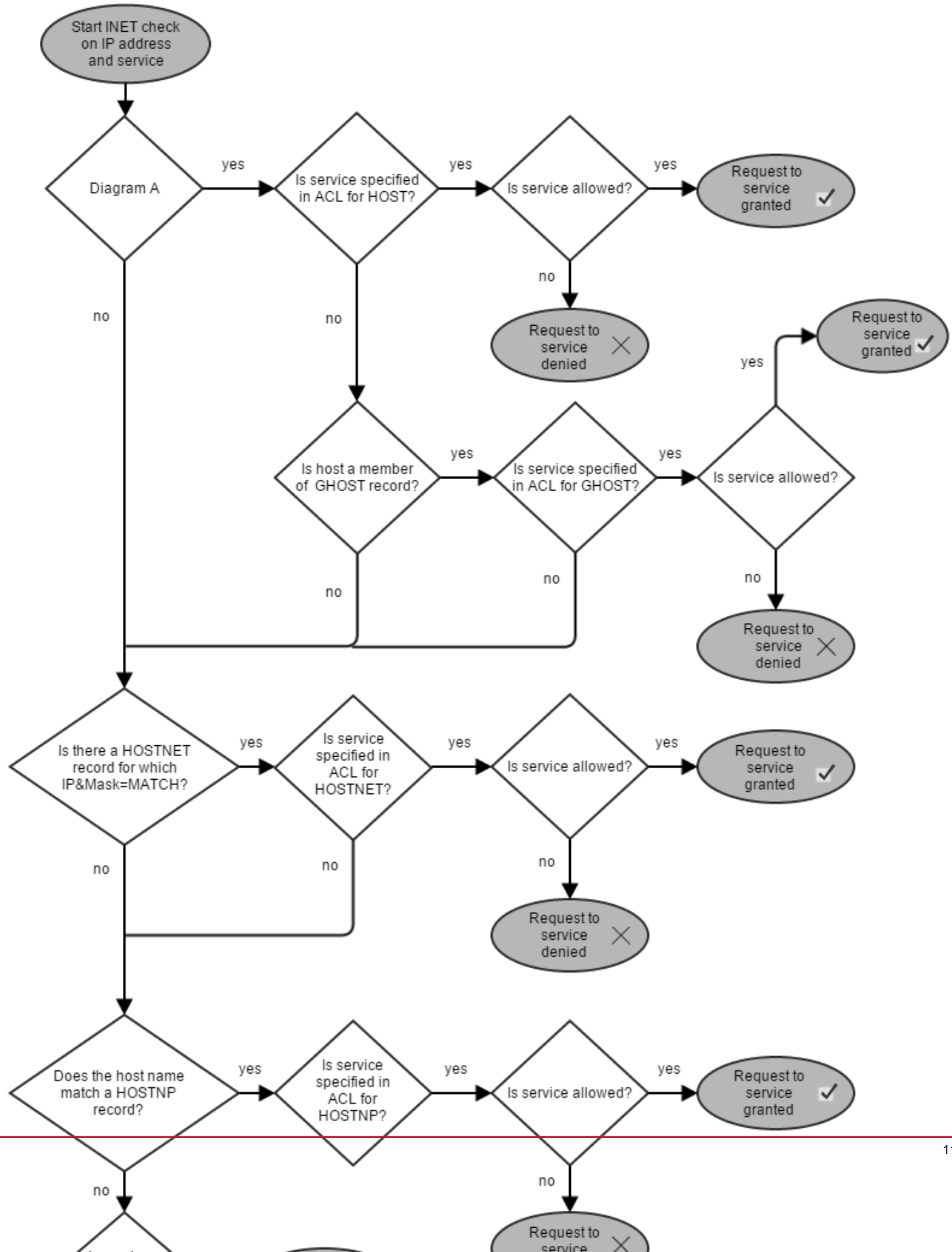
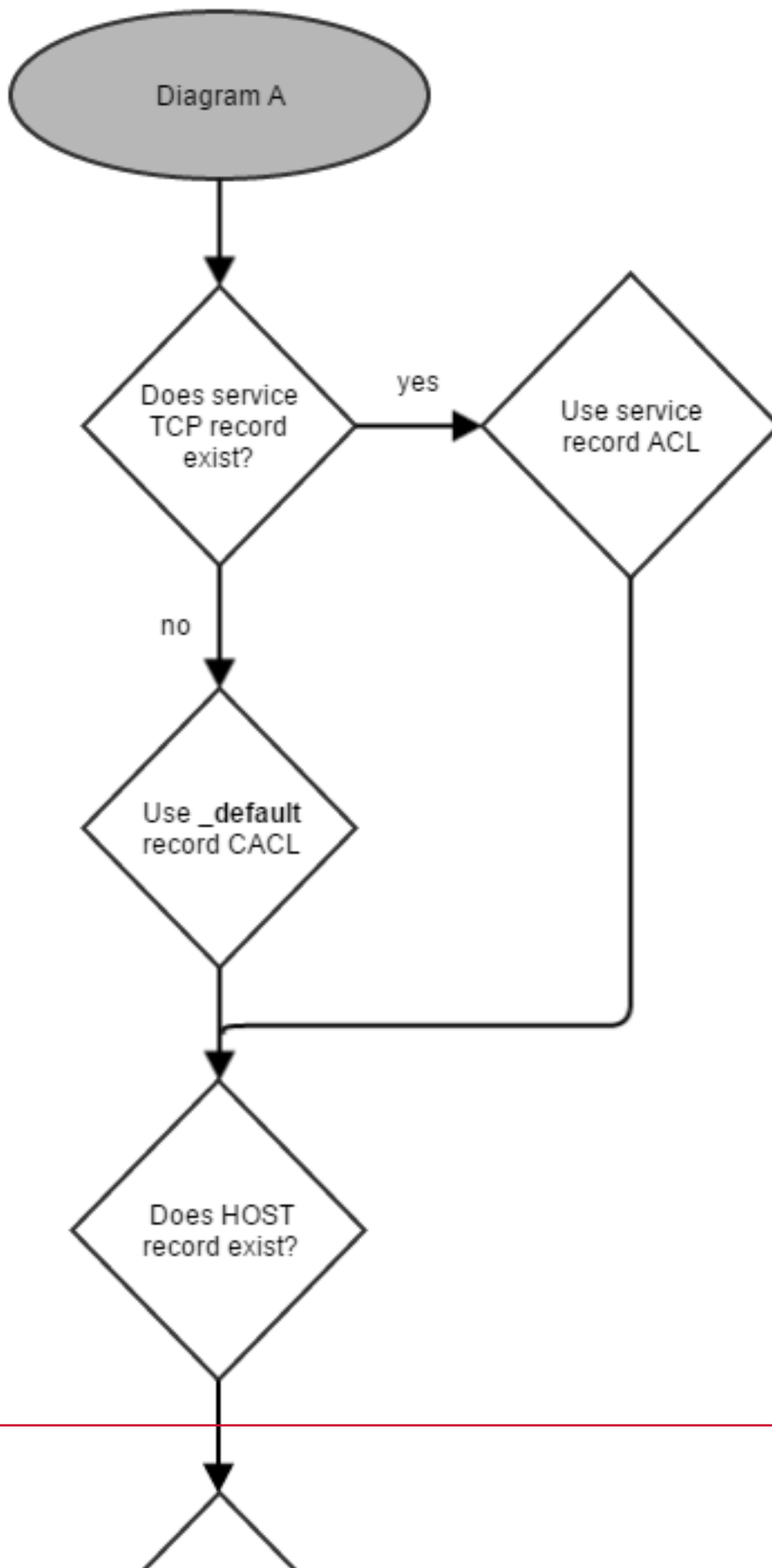


Figure 40: Incoming Authorization 2



The algorithm for outgoing authorizations is:

Figure 41: Outgoing Authorization

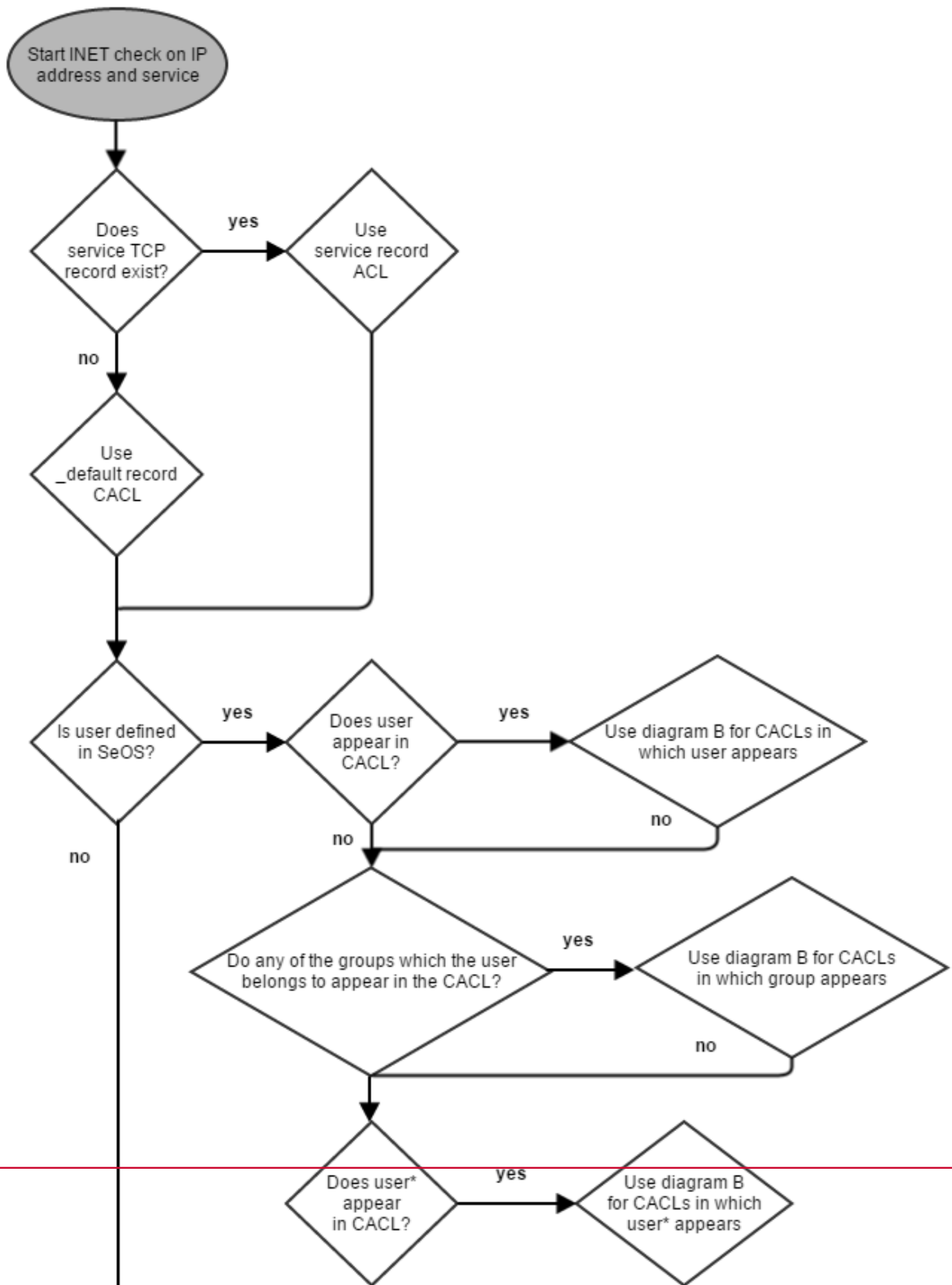
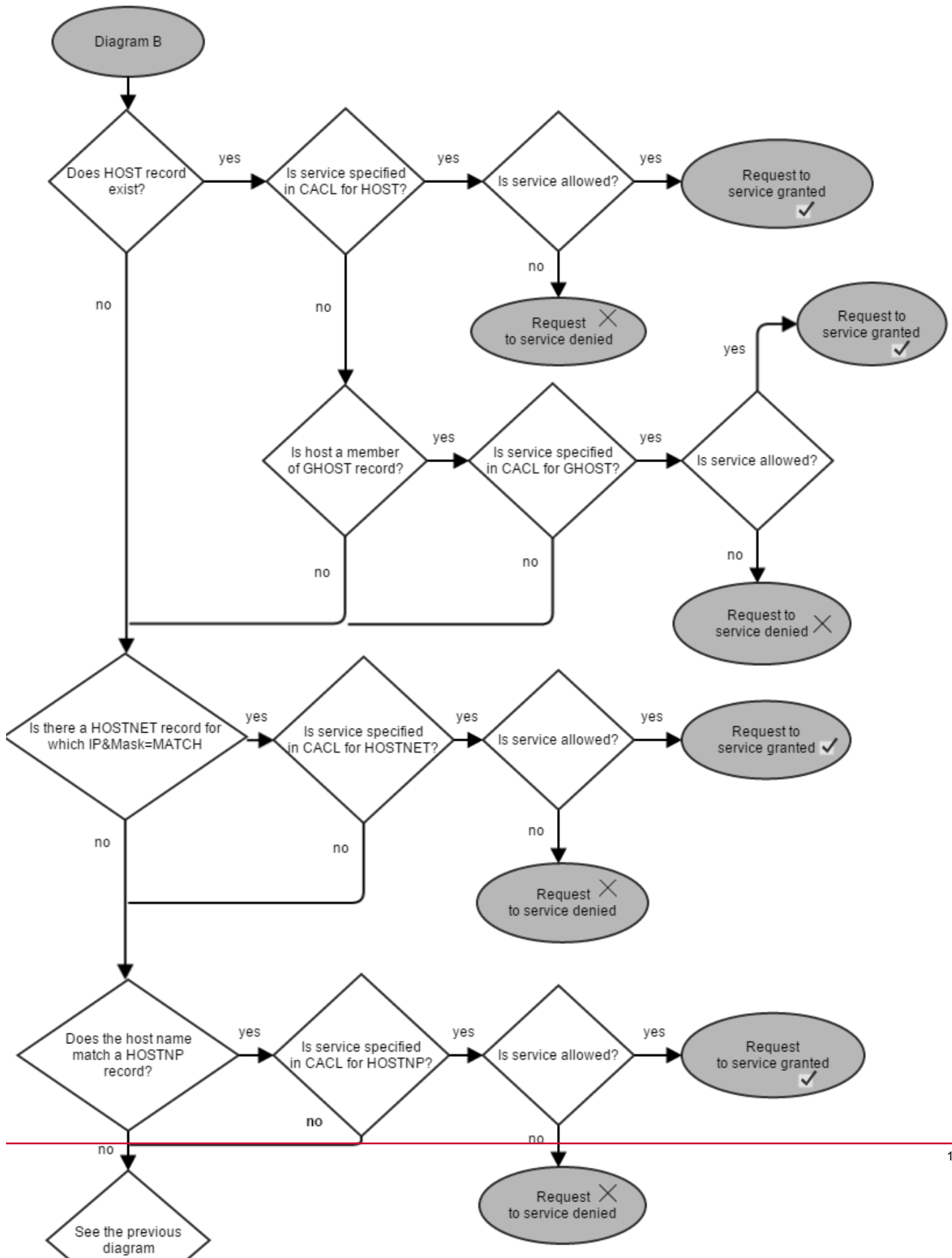


Figure 42: Outgoing Authorization 2





## Policy Model Database (UNIX)

Managing tens or hundreds of databases individually is not practical. Privileged Access Manager supplies the Policy Model service, a component that lets you manage many databases from one central database. Using the Policy Model service is optional, but it greatly simplifies administration at large sites.

The Policy Model (PMD) service uses a Policy Model database (PMDB). Like other Privileged Access Manager databases, the PMDB contains users, groups, protected resources, and rules governing access to the resources. In addition, the PMDB contains a list of *subscriber* databases. Each subscriber is a Privileged Access Manager database that resides on a separate computer, or another PMDB that resides on the same or another computer. A PMDB that updates a subscriber is the *parent* of the subscriber.

The PMDB is a useful tool for managing many databases that have similar authority restrictions and access rules.

### NOTE

For information about administrating a PMDB (sepmd utility), see the *Reference Guide*. For information about managing PMDBs remotely using selang, see the *selang Reference Guide*.

## Configure Automatic Rule-based Policy Updates

Single-rule policy updates (regular selang rules) you make in a central database are automatically propagated to the subscriber databases. By subscribing several computers to the same database, and by subscribing one database to another, you can create a hierarchy. You configure your environment for automatic rule-based policy updates after installation.

### NOTE

This method of managing policies is limited to letting you make single-rule policy updates across your hierarchy. Other functionality is only available through implementing advanced policy management and reporting.

## How Automatic Rule-based Policy Updates Work

When you configure your environment for automatic rule-based policy updates, each rule you define in the central database is automatically propagated to all its subscribers in the following way:

1. A rule is defined for any PMDB with at least one subscriber.
2. The PMDB sends the command to all subscriber databases.
3. The subscriber database applies the propagated command.
4. If the subscriber database does not respond, the PMDB sends the command at a regular interval (by default, every 30 minutes) until the subscriber database has been updated.

Alternatively, you can update subscriber databases when they become available, by setting the pull\_option token to yes in the [pmd] section of the seos.ini file on the subscriber computer.

1. If a subscriber database is responding, but refuses to apply the command, the PMDB places the command in the [Policy Model error log](#) (see page).
2. If the subscriber database is a parent to other subscribers, it then sends the command to its subscribers.

### Example: Removing a user from all computers in a hierarchy

If a user is deleted from a PMDB using the rmusr command, the same rmusr command is sent to all the subscriber databases. In this way, a single rmusr command can remove a user from many databases on various computers.

## How You Can Set Up a Hierarchy

Privileged Access Manager uses the Policy Model service to propagate rule-based policy updates across the configured hierarchy. By subscribing several Privileged Access Manager computers to the same PMDB, and by subscribing one PMDB to another, you create a hierarchy.

To enable automatic rule-based policy updates, do the following:

1. Create and configure the master PMDB.
2. (Optional) Create and configure subscriber PMDBs.
3. [Define parent PMDBs for the subscribing computers](#) (see link), called *endpoints*.

### NOTE

The following sections show how you set up a PMDB hierarchy. There are other ways of creating PMDBs and then setting their hierarchy. For a comprehensive discussion of the Policy Model utilities, see the *Reference Guide*.

## Create and Configure the Master PMDB

To let you manage policies from a central location, you first create and configure a master PMDB. On a local host, you can use the `sepmdbadm` command.

### NOTE

The following procedure shows the interactive form of the `sepmdbadm` command. For information about using the command-line parameters for all input, see the *Reference Guide*.

### Follow these steps:

1. In a command line, enter the following command:

```
sepmdbadm i
```

Privileged Access Manager starts the Policy Model database administration script (`sepmdbadm`) and displays a menu with options for you to choose from.

2. Enter 1, to select the first option (create a master PMDB and define its subscribers).

The script is configured to ask you the relevant questions.

3. Press Enter to continue.

The script continues to ask you the first question.

### NOTE

If Privileged Access Manager is not running, the script issues a warning and lets you start Privileged Access Manager before the script is rerun.

4. Enter a name for the Policy Model you want to create.

The script registers the Policy Model name and continues.

### NOTE

The first character for a PMDB name should consist of the alphanumeric characters "-" and "\_".

5. Enter the name of the first subscriber computer you want to specify.

The script registers the name of the first subscriber and then asks you to enter the name of the next subscriber.

6. Continue to enter subscriber names as necessary, then press Enter without entering a subscriber name.

The script registers all subscriber names and continues.

**NOTE**

You still must point each subscriber computer to its parent PMDB.

7. If you are running NIS, NIS+, or DNS, choose whether you want to update the NIS/DNS tables with PMDB changes.

Updates are made to users and groups in the PMDB. The tables provide information on users and their characteristics. If you choose yes, a UNIX user or UNIX group that is updated through the Policy Model is also updated in the NIS passwd and group files.

8. Enter **y** if you want to update the NIS/DNS tables.

The script now asks you for the location of the NIS passwd and group files.

9. Enter the full path of the NIS password file.

The script registers the full path and continues.

10. Enter the full path of the NIS group file.

The script registers the full path and continues.

11. Enter **n** or press Enter if you want to update the NIS/DNS tables.

The script registers your answer and continues.

12. Enter the users that you want to give special attributes for the PMDB:

13. Enter Privileged Access Manager administrator names as necessary, then press Enter without entering an administrator name.

Administrators are authorized to change the properties of the PMDB.

**NOTE**

At least one administrator must be defined in a PMDB (*root* is the default).

14. Enter enterprise user administrator names as necessary, then press Enter without entering an administrator name.

15. Enter Privileged Access Manager auditor names as necessary, then press Enter without entering an auditor name.

Auditors are authorized to view the PMDB audit log files

16. Enter enterprise user auditor names as necessary, then press Enter without entering an auditor name.

17. Enter Privileged Access Manager password manager names as necessary, then press Enter without entering a password manager name.

18. Enter enterprise user password manager names as necessary, then press Enter without entering a password manager name.

Password managers are authorized to change passwords in the PMDB.

The script registers your answer and continues.

19. Enter administration terminals as necessary, then press Enter without entering an administration terminal.

The script registers all administration terminals and then reports the selections that you have made and asks you to confirm them.

20. Press Enter to confirm the selections you have made, or enter **n** to rerun the script with new inputs.

If you confirm your selections, a new PMDB is created using the answers that you supplied.

**More information:**

[Define Parent PMDBs for Subscribing Computers](#)

## Create and Configure Subscriber PMDBs

Once you have a master PMDB configured, if you want to extend your hierarchy, create and configure subscriber PMDBs. On a local host, you can use the `sepmdadm` command.

### NOTE

The following procedure shows the interactive form of the `sepmdadm` command. For information about using the commandline parameters for all input, see the *Reference Guide*.

### Follow these steps:

1. In a command line, enter the following command:

```
sepmdadm i
```

Privileged Access Manager starts the Policy Model database administration script (`sepmdadm`) and displays a menu with options for you to choose from.

2. Enter 2, to select the second option (create a subsidiary PMDB and define its subscribers and parent.).

The script is configured to ask you the relevant questions.

3. Press Enter to continue.

The script continues to ask you the first question.

4. Enter a name for the Policy Model you want to create.

The script registers the Policy Model name and continues.

5. Enter the name of the first subscriber computer you want to specify.

The script registers the name of the first subscriber and then asks you to enter the name of the next subscriber.

6. Continue to enter subscriber names as necessary, then press Enter without entering a subscriber name.

The script registers all subscriber names and continues.

**Note:** You still must [point each subscriber computer to its parent PMDB](#).

7. Enter the name of the parent PMDB.

The script registers the parent PMDB name and continues.

### NOTE

`sepmdadm` only lets you enter one parent for each subscribing database. You can, however, define multiple parents for each database. To do this, modify the `parent_pmd` token of the `pmd.ini` configuration file. For more information about using this token, see the *Reference Guide*.

8. If you are running NIS, NIS+, or DNS, choose whether you want to update the NIS/DNS tables with PMDB changes.

Updates are made to users and groups in the PMDB. The tables provide information on users and their characteristics. If you choose yes, a UNIX user or UNIX group that is updated through the Policy Model is also updated in the NIS `passwd` and group files.

9. Enter **y** if you want to update the NIS/DNS tables.

The script now asks you for the location of the NIS `passwd` and group files.

10. Enter the full path of the NIS password file.

The script registers the full path and continues.

11. Enter the full path of the NIS group file.

The script registers the full path and continues.

12. Enter **n** or press Enter if you want to update the NIS/DNS tables.

The script registers your answer and continues.

13. Enter the users that you want to give special attributes for the PMDB:

14. Enter Privileged Access Manager administrator names as necessary, then press Enter without entering an administrator name.

Administrators are authorized to change the properties of the PMDB.

#### **NOTE**

At least one administrator must be defined in a PMDB (*root* is the default).

15. Enter enterprise administrator names as necessary, then press Enter without entering an administrator name.

16. Enter Privileged Access Manager auditor names as necessary, then press Enter without entering an auditor name.

Auditors are authorized to view the PMDB audit log files.

17. Enter enterprise user auditor names as necessary, then press Enter without entering an auditor name.

18. Enter Privileged Access Manager password manager names as necessary, then press Enter without entering a password manager name.

Password managers are authorized to change passwords in the PMDB.

19. Enter enterprise user password manager names as necessary, then press Enter without entering a password manager name.

The script registers your answer and continues.

20. Enter administration terminals as necessary, then press Enter without entering an administration terminal.

The script registers all administration terminals and then reports the selections that you have made and asks you to confirm them.

21. Press Enter to confirm the selections you have made, or enter **n** to rerun the script with new inputs.

If you confirm your selections, a new PMDB is created using the answers that you supplied.

### **Define Parent PMDBs for Subscribing Computers**

To establish an endpoint computer as a subscriber to a PMDB, you must do more than register the subscriber's name in the PMDB. You also need to complete a procedure at the subscriber computer.

#### **To define parent PMDBs for subscribing computers**

1. In a command line on the subscriber computer, start `sepmdadm` in interactive mode:

```
sepmdadm i
```

Privileged Access Manager starts the Policy Model database administration script (`sepmdadm`) and displays a menu with options for you to choose from.

2. Enter 3, to select the third option (define the parent and password PMDBs of the local host).

The script is configured to ask you the relevant questions.

3. Press Enter to continue.

The interactive script continues to ask you the first question.

**NOTE**

If Privileged Access Manager is running, the script issues a warning and lets you stop Privileged Access Manager before the script is rerun.

4. Enter the name of the parent PMDB.

The script registers the name of the parent PMDB name and continues.

5. Enter the name of the parent password PMDB.

The script registers the name of the parent password PMDB name and then reports the selections you have made and asks you to confirm them.

6. Press Enter to confirm the selections you have made, or enter **n** to rerun the script with new inputs.

If you confirm your selections, the subscriber computer is set up with these inputs.

**NOTE**

sepmdadm only lets you enter one parent for each subscribing database. You can, however, define multiple parents for each database. To do this, modify the parent\_pmd token of the seos.ini configuration file. For more information about using this token, see the *Reference Guide*.

**How You Use a PMDB to Propagate Configuration Settings**

When you edit a Policy Model's configuration, the new configuration values are propagated to the Policy Model's subscribers.

The following process describes how configuration updates are propagated to a Policy Model's subscribers:

1. You edit one or more of the Policy Model's configuration values.
2. The Policy Model writes the new configuration values to the virtual configuration file.

**Note:** The virtual configuration file does not contain values for the audit.cfg file. The Policy Model does not write any changes that you make to this file to the virtual configuration file.

1. The Policy Model sends the new configuration values to its subscribers.
2. selang commands update each subscriber with the new configuration values.

**Virtual Configuration File**

Each Policy Model has a virtual configuration file that contains the configuration values for its subscribers. The virtual configuration file is located in the PMD directory, and is named `cfg_configname`, where *configname* is the name of the Policy Model configuration.

The virtual configuration file does not contain the configuration values held in the audit.cfg file.

**How New Subscribers Are Configured**

The Policy Model configures each new subscriber with the existing configuration values. The existing configuration values are stored in the virtual configuration file.

**Note:** The virtual configuration file does not store configuration values from the audit.cfg file. Any changes that you make to the audit.cfg file before creating a subscriber are not propagated to the new subscriber.

The following process describes how a Policy Model configures new subscribers:

1. You create a subscriber to the Policy Model.
2. The Policy Model reads the values in its virtual configuration file.
3. The Policy Model adds the configuration values from its virtual configuration file to the updates.dat file. The updates.dat file also contains the access rules for the Policy.
4. The Policy Model sends the updates.dat file to the new subscriber.

5. `selang` commands configure the new subscriber with the values in the `updates.dat` file.

## UID/GID Synchronization

As an administrator, you receive messages that refer to users by UID and to groups by GID. Verify that the UIDs and GIDs have the same meaning everywhere.

By default, the PMDB attempts to use the same UIDs and GIDs for new users and groups everywhere. You can help by providing the necessary conditions from the start as follows:

- Start with identical `passwd` files and identical group files.
- Make sure that the `synch_uid` token in the `pmd.ini` file is set to yes.

You can depend on compatibility between the UIDs and between the GIDs of your local database, your PMDB, and your PMDB subscribers if the following conditions exist:

- Your local database is a subscriber to your PMDB
- The PMDB is the only source of new users and new groups for your subscriber databases

If you create a user with a UID that is already in use in the PMDB or in some other subscriber computer, the individual update of the subscriber fails. In all other subscriber computers where no such conflict exists, the update succeeds.

An alternative to synchronizing your `passwd` and group files is to specify the UID of each new user and the GID of each new group explicitly.

## Synchronize Users and Groups

To ensure the lists of users and groups in your various databases correspond correctly at all times, you need an initial set of identical lists. Because the password and group files are so important, synchronize them before they begin accumulating local user and group information.

### To synchronize users and groups

1. Copy your `/etc/passwd` file and `/etc/group` file to your Policy Model directory.

This is a onetime procedure that destroys any previous `passwd` and group files in your [Policy Model directory](#).

#### NOTE

If you are using a shadow file and want to synchronize passwords, we recommend using the `secrepsw` utility. For more information, see the *Reference Guide*

2. Copy the `/etc/passwd` file and `/etc/group` file to each subscriber computer so that they are identical to the ones on your own computer.

3. On the computer where the PMDB resides, ensure that the `synch_uid` token in your `pmd.ini` file is set to yes.

By default, the value of the token `synch_uid` is yes. If you ever want a subscriber database to have independent default UIDs and default GIDs (that is, not necessarily attempting to match those of the PMDB), you can set `synch_uid` to no.

## Specify UIDs Explicitly

Another way to send an identical UID or GID to the PMDB and to all its subscribers is to explicitly set it when you create a new user.

To specify UIDs explicitly, use the `userid` or `groupid` parameter with each `newusr` command.

### Example: Create a new user with a specified UID

If you want to establish 1234 explicitly as the UID of new user `terry_jones` (and assuming that no one else in the database has that UID yet), enter the command:

```
newusr terry_jones unix (userid(1234))
```

If the specified UID is already being used in the PMDB, then the PMDB will not itself be updated, but the command will still propagate to the other subscriber databases. Among the other databases, wherever the particular UID is already in use, the subscriber's individual update will fail; but where no such conflict exists, the update succeeds.

## How the Policy Model Updates Subscribers

When updating subscribers, the Policy Model performs the following actions:

1. The Policy Model tries to qualify subscriber names fully as they are added to or deleted from the Policy Model.
2. The PMDB daemon, `sepmdd`, attempts to update a subscriber database for the amount of time defined by the token `QD_timeout`.
3. If the maximum time elapses and the daemon does not succeed in updating a subscriber, it skips that particular subscriber. The daemon then tries to update the remainder of the subscribers on its list.
4. After it completes its first scan of the subscriber list, `sepmdd` performs a second scan. In the second scan, `sepmdd` tries to update the subscribers that it did not succeed in updating during its first scan. During the second scan, it tries to update a subscriber until the connect system call times out (approximately 90 seconds).

### NOTE

The token `QD_timeout` may be found in both the `seos.ini` and `pmd.ini` files. If the token exists in both files, `sepmdd` uses the value in the `pmd.ini` file.

Whenever a PMDB encounters an error while propagating updates to subscribers, the `sepmdd` daemon creates an entry in the [Policy Model error log file](#) (see link). This file, `ERROR_LOG` by default, is located in the [PMDB directory](#).

## Clean Up the Update File

The `sepmdd` utility automatically writes each update it receives in the `updates.dat` file. To prevent the file from growing too large, we recommend that you delete processed updates from the file periodically.

To clean up the update file, use the following command:

```
sepmdd t pmdbName auto
```

`sepmdd` calculates the offset of the first update entry that has not been propagated and deletes all the update entries before it.

### NOTE

For more information about `sepmdd` utility, see the *Reference Guide*.

## Encrypt the Update File

After you create a PMDB, but *before* you start `sepmdd`, you can specify that information saved to the `updates.dat` file be encrypted.

To encrypt the update file, set the `UseEncryption` token to `yes` in the `[pmd]` section of the `pmd.ini` file.

To decrypt the `updates.dat` file, use the `sepmdd` utility with the `de` switch.

### NOTE

For more information about `sepmdd`, see the *Reference Guide*.



## Exclude Subscribers

You can skip subscribers so that they do not receive updates from parent PMDBs.

To exclude the local host, set the token `exclude_localhost` to `yes` in the `pmd.ini` file.

To add additional subscribers to the excluded list, set the token `exclude_file` (*name of file*).

To make a subscriber receive updates, remove the subscriber from the excluded list.

## Filter Updates

If you want your PMDB to update different subsets of data at different subscriber databases, you need to define which records are sent to subscriber databases.

### To filter updates

1. [Configure PMDBs to serve as parents to subsets of subscribers.](#)
2. Modify the *filter* token in the `pmd.ini` file of the parent PMDB to point to a filter file you set up on the same computer.

Updates to the subscriber databases are then limited to the records that pass the filter.

### NOTE

When you execute a `join` or `join- selang` command in the native UNIX environment, Privileged Access Manager changes the command to `change group (cg)`. To filter `join` or `join-` commands in the native UNIX environment, use the following line in the filter file:

```
MODIFY UNIX GROUP GroupName USERS NOPASS
```

You cannot filter `join` or `join-` commands by user name in the native UNIX environment. This rule does not apply to `join` or `join-` commands in any other environment.

## Policy Model Error Log File

The Policy Model error log, which is organized chronologically, looks similar to this:

| Error Text                                                                                                                                                                                                                              | Error Category         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| 20 Nov 03 11:56:07 (pmdb1): fargo nu u5 0 Retry<br>ERROR: Login procedure failed (10068)<br>ERROR: Cannot accept update from a nonparent PMDB<br>(pmdb1@name.company.com) (10104)                                                       | Configuration Errors   |
| 20 Nov 03 19:53:17 (pmdb1): fargo nu u5 0 Retry<br>ERROR: Connection failed (10071)<br>Host is unreachable (12296)                                                                                                                      | Connection Errors      |
| 20 Nov 03 11:57:06 (pmdb1): fargo nu u5 560 Cont<br>ERROR: Failed to create USER u5 (10028)<br>Already exists (9)<br>20 Nov 03 11:57:06 (pmdb1): fargo nu u5 1120 Cont<br>ERROR: Failed to create USER u5 (10028)<br>Already exists (9) | Database Update Errors |

The Policy Model error log is in binary format; you can view it only by entering the following command:

```
ACInstallDir/bin sepmd e pmdname
```

### NOTE

Do not manually delete an error log (for example, with the UNIX `rm` command). To delete the log, only use the following command:

```
ACInstallDir/bin sepmd c pmdname
```

**WARNING**

The error log in Privileged Access Manager r5.1 and later versions has a format that is not compatible with the format of earlier versions. sepmdd cannot handle error logs from these earlier versions. When you upgrade to a version that has this format, the old error log is copied to ERROR\_LOG.bak; a new log file is created when you start sepmdd.

**Example: PMDB Update Error Message**

The following example shows a typical error message:

```

date      time      pmdb name      subscriber      command      offset      flag
  ↓          ↓          ↓          ↓          ↓          ↓          ↓
20 Nov 03 19:53:17 (pmdb1): fargo nu u5 0 Retry
ERROR: Connection failed (10071) ← major level (type of error)
Host is unreachable (12296) ← minor level (cause of error)
                        ↑
                    return code

```

- The top line always consists of the date, time, and subscriber. The command that generated the error appears next, followed by the offset (in decimal format), which indicates the location of the failed update inside the updates file. Lastly, the flag indicates whether the PMDB retries the update automatically or continues without it.
- The second line shows an example of a major level message (what type of error occurred) and its return code.
- The third line displays an example of a minor level message (why the error occurred), and its return code.

**Example: Error Message**

A command may generate and display more than one error. Also, an error may consist of a major level message, a minor level message, or both.

The following error has only one message level:

```
Fri Dec 29 10:30:43 2003 CIMV_PROD:Release failed. Return code = 9241
```

This message occurs when sepmdd pull attempts to release a subscriber that is already available.

**Policy Model Filter File**

A filter file consists of lines, each with six fields. The fields contain information about:

- The form of access that is permitted or denied.  
For example, READ or MODIFY
- The environment that is affected:  
For example, AC or native
- The class of the record.  
For example, USER or TERMINAL
- The objects, within the class, that the rule covers.  
For example, User1, AuditGroup, or TTY1
- The properties that the record grants or cancels.

For example, OWNER and FULL\_NAME in the filter line means that any command having those properties is filtered. You must enter each property exactly as it appears in the *Reference Guide*.

- Whether such records should be forwarded to the subscriber database or not:

PASS or NOPASS

The following rules apply to each line in the filter file:

- You can use an asterisk \* to denote all possible values in any field.
- If more than one line covers the same records, the *first* applicable line is used.
- Spaces separate the fields.
- In fields with more than one value, semicolons separate the values.
- Lines beginning with # are considered comment lines.
- Empty lines are not allowed.

#### Example: Filter file

The following example describes a line from a filter file:

|                |             |       |                      |                    |           |
|----------------|-------------|-------|----------------------|--------------------|-----------|
| CREATE         | AC          | USER  | *                    | FULL_NAME;OBJ_TYPE | NOPASS    |
| form of access | environment | class | record name( * =all) | properties         | treatment |

In this example, if we name the file with this line TTY1\_FILTER and edit the pmd.ini file for PMDB TTY1 so that filter=/opt/CA/PAMSC/TTY1\_FILTER, then PMDB TTY1 does not propagate to its subscribers any records that create new users with the FULL\_NAME and OBJ\_TYPE property.

### Propagate Passwords

When a user changes a password using the sepass utility, the new password is normally sent to the computer's parent PMDB. The parent PMDB is defined in the parent\_pmd or the passwd\_pmd token in the [seos] section of the seos.ini file or in both. However, if the user changes the password with the utility sepass, you can also specify that the user's new password should be sent to and propagated by a separate PMDB.

To send a new user's password to a separate PMDB, use the pmd parameter with the newusr, chusr, or editusr command.

#### Example: Specifying a separate PMDB for password propagation

To specify that the new passwords created with sepass for the user Tony should be sent to and propagated by a separate PMDB pw\_pmd@name1.yourorg.com, enter the following command:

```
editusr tony pmd(pw_pmd@name1.yourorg.com)
```

### Remove a Subscriber

If you no longer want to propagate updates to a particular subscriber, remove it. Alternatively, you can [exclude a subscriber from receiving updates](#).

#### To remove a subscriber

1. Remove the computer from the subscription list:

```
sepm u PMDB_name computer_name
```

The computer is removed from the Policy Model subscription list.

2. Shut down seosd on the computer that you removed from the subscription list:

```
secons -s
```

The daemon seosd is shut down.

3. Delete the value of the parent\_pmd token in the [seos] section of the seos.ini file on the computer you removed from the subscription list.

The computer will stop accepting updates from the parent PMDB.

4. Restart seosd.

The active database on the computer that you removed from the subscription list is no longer a subscriber of the specified PMDB.

#### NOTE

Once the database is unsubscribed from the PMDB, the PMDB no longer sends commands.

### Update a Policy Model Database

Working at the computer where the PMDB resides does not automatically update the PMDB itself. To update a PMDB, specify it as your target database.

To specify a target database, use the hosts command in the selang command shell:

```
hosts pmd_name@pmd_host
```

All selang commands now update the policy model database specified. The commands then automatically propagate to the active databases on this computer and of all subscriber computers.

#### Example: Specify a target PMDB

To set the target database to policy1 on myPMD\_host, use the following command:

```
hosts policy1@myPMD_host
```

If you now enter the newusr command, the new user is added to the policy1 database. The new user is also added to the active databases on this computer and all subscriber computers.

### Policy Model Backup

When you back up a PMDB, you copy the data in the Policy Model database to another directory. This includes:

- Policy information
- The list of the Policy Model's subscribers
- Configuration settings
- Registry entries
- The updates.dat file

You cannot restore a PMDB from backup files that use another platform, operating system, or version of Privileged Access Manager. Ensure you back up the Policy Model to a host running the same platform, operating system, and version of Privileged Access Manager.

### Back Up a PMDB Using sepmd

When you back up the PMDB, you copy the data from the Policy Model database to a specified directory. You should store the backed up PMDB files in a secure location, preferably protected by Privileged Access Manager access rules.

You can use the sepmd utility to back up a PMDB on a local host. You can also use selang commands to back up a PMDB on a remote host.

**Note:** You can back up a PMDB recursively. A recursive backup backs up all the PMDBs in a hierarchy to the host you specify, and modifies the PMDB subscribers so that the subscription still works when the backup is moved to the host. You can only use a recursive backup if the master and child PMDBs are deployed on the same host.

#### To back up a PMDB using sepmd:

1. Lock the PMDB using the following command:

```
sepmd -bl pmdb_name
```

The PMDB is locked and cannot send commands to its subscribers.

2. Do one of the following:

- Back up the PMDB using the following command:

```
sepmdb -bh pmdb_name [destination_directory]
```

- Back up the PMDB recursively using the following command:

```
sepmdb -bh pmdb_name [destination_directory] [backup_host_name]
```

### NOTE

If you do not specify a destination directory, the backup is saved to the following directory:  
*ACInstallDir\data/policies\_backup/pmdb\_name*

3. Unlock the PMDB using the following command:

```
sepmdb -ul pmdb_name
```

The PMDB is unlocked and can send commands to its subscribers.

## Back Up a PMDB Using selang

When you back up the PMDB, you copy the data from the Policy Model database to a specified directory. You should store the backed up PMDB files in a secure location, preferably protected by Privileged Access Manager access rules. You can use selang commands to back up a PMDB on a local or remote host. You can also use the sepmdb utility to back up a PMDB on a local host.

### NOTE

You can back up a PMDB recursively. A recursive backup backs up all the PMDBs in a hierarchy to the host you specify, and modifies the PMDB subscribers so that the subscription still works when the backup is moved to the host. You can only use a recursive backup if the master and child PMDBs are deployed on the same host.

### Follow these steps:

1. (Optional) If you are using selang to connect to the PMDB from a remote host, connect to the PMDB host using the following command:

```
host pmdb_host_name
```

2. Move to the PMD environment using the following command:

```
env pmd
```

3. Lock the DMS using the following command:

```
pmd pmdb_name lock
```

The PMDB is locked and cannot send commands to its subscribers.

4. Back up the DMS database using the following command:

```
backuppmd pmdb_name [destination(destination_directory)] [hir_host(host_name)]
```

### NOTE

If you do not specify a destination directory, the backup is saved to the following directory:  
*ACInstallDir\data/policies\_backup/pmdbName*

5. Unlock the PMDB using the following command:

```
pmd pmdb_name unlock
```

The PMDB is unlocked and can send commands to its subscribers.

## Policy Model Restoration

When a Policy Model is restored, Privileged Access Manager copies the backup PMDB files into the specified directory. Everything that is in the original PMDB files is copied to the new PMDB directory, including:

- Policy information
- The list of the Policy Model's subscribers
- Configuration settings
- registry entries
- The updates.dat file

If there is an existing PMDB in the destination directory, Privileged Access Manager deletes the existing files before copying the restoration files into that directory.

You cannot restore a PMDB from backup files that use another platform, operating system, or version of Privileged Access Manager. Ensure you back up the Policy Model to a host running the same platform, operating system, and version of Privileged Access Manager.

## Restore a PMDB

When you restore a PMDB, Privileged Access Manager copies the data from the PMDB backup files into the directory you specify. Privileged Access Manager must be running on the terminal you do the restoration on.

**Note:** If you back up and restore the PMDB on different terminals, the PMDB does not automatically update the terminal resource in the restored PMDB database. You must add the new terminal resource to the restored PMDB. To add the new terminal resource, stop the restored PMDB, run the *selang -p pmdb* command, then start the restored PMDB.

To restore a PMDB, run *one* of the following on the terminal that you want to restore the PMDB on:

- *sepmc -restore* utility
- *selang restore pmd* command

### NOTE

For more information about the *sepmc* utility, see the *Reference Guide*. For more information about *selang* commands, see the *selang Reference Guide*.

## Architecture Dependency

When deploying Privileged Access Manager, consider the hierarchy of your environment. At many sites, the network includes various architectures. Some policy rules, such as the list of trusted programs, are architecture-dependent. On the other hand, most rules are independent of the system architecture.

You can cover both kinds of rules by using a hierarchy. Define a global database for architecture-independent rules, and give it subscriber PMDBs that define architecture-dependent rules.

### NOTE

The root PMDB and all its subscribers can reside on the same computer or on separate computers, depending on the physical needs of your environment.

## Example: A Two-tiered Deployment Hierarchy

The following UNIX example also applies to a Windows architecture with small modifications.

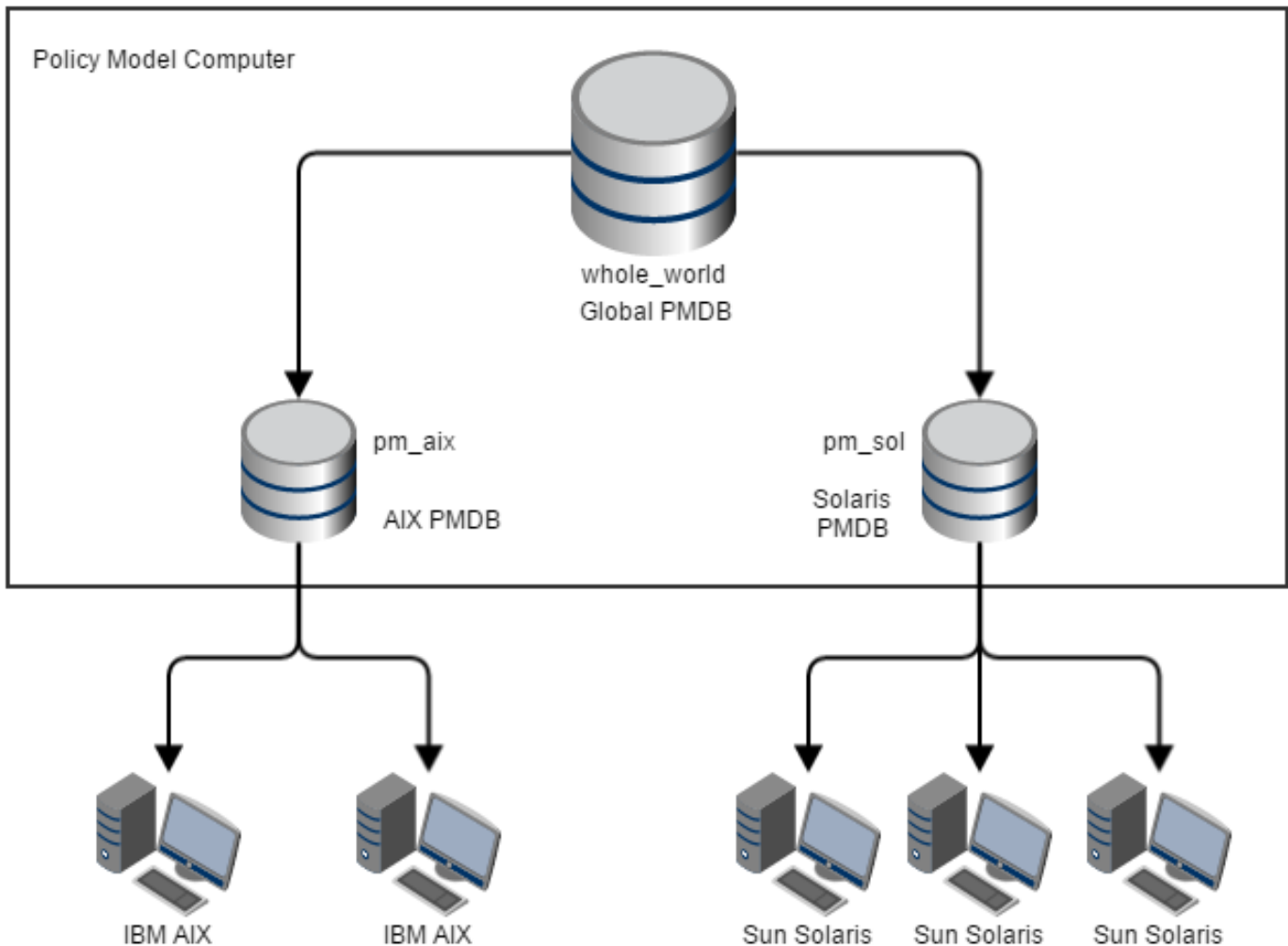
In the example, the site consists of IBM AIX and Sun Solaris systems. Since the list of trusted programs on IBM AIX differs from the one on Sun Solaris, the PMDBs need to consider architecture dependency.

To set up a multiple-architecture PMDB, set up your PMDBs as follows:

1. Define a PMDB named `whole_world`, to contain the users, groups, and all other architecture independent policies.
2. Define a PMDB named `pm_aix`, to contain all the IBM AIX specific rules.
3. Define the PMDB `pm_sol`, to contain all the Sun Solaris specific rules.

The PMDBs `pm_aix` and `pm_solaris` are subscribers of the PMDB `whole_world`. All IBM AIX computers at the site are subscribers of `pm_aix`. All Sun Solaris computers at the site are subscribers of `pm_sol`. The concept is illustrated in the following chart:

**Figure 43: Architecture dependency**



4. When you enter platform-independent commands in `whole_world`, such as adding a user or setting a SURROGATE rule, all databases at the site are automatically updated.

5. When you add a trusted program to `pm_aix`, only IBM AIX computers are updated, without affecting the Sun Solaris systems.

## Manage Local PMDBs

Privileged Access Manager offers several utilities for administering local PMDBs:

### **sepmdb**

A PMDB administration utility that lets you:

- Administer subscribers
- Truncate the update file
- Administer Dual Control
- Manage the Policy Model log file
- Perform other administrative tasks

### **sepmdbadm**

Creates PMDBs and configures them with the necessary settings for setting up your hierarchy.

#### **NOTE**

The root PMDB and all of its subscribers can reside on the same computer or on separate computers, depending on the physical needs of your environment.

## Manage Remote PMDBs

Privileged Access Manager offers a range of selang commands that you can use in the pmd environment. These commands let you manage PMDBs remotely:

### **backuppmd**

Backs up a PMDB.

### **createpmd**

Creates a PMDB.

### **deletepmd**

Deletes a PMDB.

### **findpmd**

Displays the names of all PMDBs on the computer.

### **listpmd**

Lists the following information about a PMDB:

- Subscribers and their status
- PMDB description and its status
- Commands in the update file and their offsets
- Contents of the error log

### **pmd**

A PMDB administration command that lets you:

- Remove a subscriber from the list of unavailable subscribers
- Clear the Policy Model error log
- Lock and unlock the Policy Model
- Start and stop the Policy Model daemon
- Truncate the update file
- Reload the initialization files

### **restorepmd**

Restores a PMDB from its backup files.



**subs**

A PMDB subscription command that lets you:

- Add an existing subscriber to a parent PMDB
- Add a new subscriber to a parent PMDB
- Assign a parent PMDB to a database (Privileged Access Manager or another PMDB)

**subspmd**

Assigns a parent PMDB to the local database.

**unsubs**

Removes a subscriber from the PMDB.

**NOTE**

For a comprehensive description of *selang* commands you can use in the *pmd* environment, see the *selang Reference Guide*.

**Methods for Centrally Managing Policies**

Privileged Access Manager lets you manage several databases from a single computer in the following ways:

- **Automatic rule-based policy updates:** Regular rules you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.

**NOTE**

Dual control is only available with this method and on UNIX only. Information about dual control for automatic rule-based policy updates is found in the *Endpoint Administration Guide for UNIX*. Information about automatic rule-based policy updates can also be found in the *Endpoint Administration Guide for Windows*.

- **Advanced policy management:** Policies (groups of rules) you deploy are propagated to all databases based on host or host group assignment. You can also undeploy (remove) policies and view deployment status and deployment deviation. You need to install and configure additional components to use this functionality.

**NOTE**

Information about advanced policy management is found in the *Enterprise Administration Guide*.

**PMDB Location on Disk**

All PMDBs reside in a common directory (one per computer). The name of the directory is specified by the *pmd\_directory* token in the [pmd] section of the *seos.ini* file. The default value of *pmd\_directory* is *ACInstallDir/policies*, where *ACInstallDir* is the installation directory for Privileged Access Manager (by default */opt/CA/PAMSC*).

Each PMDB occupies a subdirectory in the common directory. The name of the subdirectory is the name of the Policy Model. The files in the subdirectory contain all the data required to define the Policy Model, including the *pmd.ini* file.

**Dual Control**

Dual Control is a way of operation that divides the process of updating the PMDB into two stages:

- Creating a transaction which consists of one or more commands.  
The *maker*--any user with the ADMIN attribute--enters one or more commands that update the PMDB. The transaction is given a unique ID number and placed in a file, where it waits to be processed before execution.
- Authorizing the transaction for execution.

The *checker*--not the same user, but any *other* user with the ADMIN attribute--locks the commands in the transaction, checks the commands, and authorizes or rejects them. If the transaction is authorized, then the commands are executed in the PMDB. If the transaction is rejected, then the transaction is deleted and the PMDB is not updated. The checker cannot authorize some of the commands in a transaction and reject others. The checker must process the transaction as a whole.

#### NOTE

Only the find and show commands do not need the authorization of a checker.

Using the parameters in the `sepmdd` utility, makers can list, retrieve and edit, or delete unprocessed transactions. Checkers can lock transactions to authorize or reject them. Checkers can also unlock transactions for processing later or by a different checker.

When the `sepmdd` daemon receives the `start_transaction` command, it sends the child process a unique number. The child process tags any further commands with this identifying number. The number is added to the new transaction and kept in the memory of the `sepmdd` daemon. When `sepmdd` receives the `end_transaction` command, the authorization algorithm is invoked. The authorization algorithm checks that none of the commands in the transaction pertain to the maker of the transaction. The algorithm also checks that none of the objects in the commands are already locked by another transaction that is waiting to be processed before execution.

You cannot use the same objects in different transactions before they are processed. If the check passes, then the relevant objects are locked, the transaction is assigned a unique sequential number, and the data is saved in a file. Each transaction is saved in a different file.

#### NOTE

For more information about the `sepmdd` utility or the `sepmdd` daemon, see the *Reference Guide*.

## Activate Dual Control

Dual Control lets you divide the duty of updating PMDBs between two people: a maker and a checker.

To activate Dual Control, set the `is_maker_checker` token, in the `pmd.ini` file *and* in the `[pmd]` section of the `seos.ini` file, to `yes`:

```
is_maker_checker=yes
```

#### NOTE

Create the Policy Model maker *before* setting these token values.

## Create or Edit Transactions

When Dual Control is activated, the maker needs to create transactions before these are processed by a checker.

### To create a transaction:

1. Ensure that the following is true:
  - You (as a maker) have the ADMIN authority.
  - None of the commands pertain to you. (You cannot enter commands that change yourself.)
  - None of the objects in the commands are already part of another transaction that has not been processed by a checker yet.
  - All the objects in the commands exist.
  - You are not editing an existing transaction that another maker invoked. (You can only edit your own transactions.)
2. Connect to the maker PMDB:

```
hosts maker@
```

The hosts command connects you to the PMDB (maker). When Dual Control is activated, the name of the PMDB is always maker. After you enter the hosts command, a message reports whether the connection to the host is successful or not.

3. Start the transaction:

```
start_transaction transactionName
```

Use the start\_transaction command as the first step when entering or updating a transaction. You can describe the transaction or can give it any name that you want, up to 256 alphanumeric characters.

4. Enter your transaction.

This is a list of commands. For example:

```
newusr mary owner(bob) audit(failure,loginfailure)
```

```
chres TERMINAL tty30 defaccess(read) \ restrictions(days(weekdays)time(0800:1800))
```

5. End the transaction:

```
end_transaction
```

The transaction is complete; you are presented with the unique ID number assigned to your transaction. The commands are placed in a file, where you can still access and change them until a checker, in preparation for processing, locks them.

**NOTE**

Make sure you record the transaction ID number if you want to be able to edit the transaction later.

**To edit a transaction:**

- When you enter the end\_transaction command, an ID number displays. This is a unique number that identifies the transaction. If you want to overwrite your transaction later, then the process is the same as creating a transaction, except that you add to the file the transaction's ID number after the name. You can enter to the file any changes you want to make. For example:

```
hosts maker@
```

```
start_transaction transactionName transactionId
```

You can then enter the appropriate commands to update the transaction:

```
chusr mary category (FINANCIAL)
```

```
end_transaction
```

- View specific unprocessed transactions with the following parameters.

Make sure you are in the *ACInstallDir/bin* path (where *ACInstallDir* is the installation directory for Privileged Access Manager, by default */opt/CA/PAMSC*).

| Command with Parameter   | Description                                                                                                                                                                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>sepmc -m l</code>  | Lists the unprocessed transactions of the user who invoked the parameter.                                                                                                                                                                                     |
| <code>sepmc -m la</code> | Lists all the transactions of all the makers that are waiting to be processed.                                                                                                                                                                                |
| <code>sepmc -m lo</code> | Lists the transactions of all the makers except those of the user who invoked the parameter<br>Each transaction in the list includes the name of the maker, the ID number of the transaction, and a description of the transaction, if the maker entered one. |

- Retrieve a specific transaction to the standard output with the following command:

```
sepmc -m r transactionId
```

- Delete a specific transaction with this command:

```
sepmc -m d transactionId
```

## Check and Process Transactions

When Dual Control is activated, the checker needs process transactions created by a maker.

### To check a transaction:

1. Make sure that the following conditions are true:
  - You (as the checker) have ADMIN authority.
  - Another Checker does not lock the transaction.
  - None of the commands pertain to you. (You cannot process commands that involve yourself.)
2. Navigate to the *ACInstallDir/bin* path  
where *ACInstallDir* is the installation directory for Privileged Access Manager, by default */opt/CA/PAMSC*.
3. View the transactions that are waiting to be processed before execution:

```
sepmc -m la
```

Or, view all the transactions except the transactions that you yourself created:

```
sepmc -m lo
```

Each transaction includes the name of the maker, the ID number of the transaction, and the name or description of the transaction.

4. Lock the transactions before processing them:

```
sepmc -m r transactionId
```

**NOTE**

A locked transaction cannot be changed.

## 5. Process the transaction:

```
sepmdd -m p transactionIdcode
```

codeCan be one of the following:

- 0—The transaction is rejected. In this case, all the commands in the transaction are deleted and no changes are implemented in the PMDB.
- 1—The transaction is authorized. The commands in the transaction are immediately implemented in the PMDB.
- 2—The transaction is unlocked. The transaction returns to the queue of waiting transactions and can be processed later, perhaps by a different checker.

```
sepmdd -m p transactionId code
```

— *code*

Can be *one* of the following:

- **0** The transaction is rejected.  
In this case, all the commands in the transaction are deleted and no changes are implemented in the PMDB.
- **1** The transaction is authorized.  
The commands in the transaction are immediately implemented in the PMDB.
- **2** The transaction is unlocked.  
The transaction returns to the queue of waiting transactions and can be processed later, perhaps by a different checker.

A message appears stating which commands were successful and which failed.

**NOTE**

For more information on makers and checkers, see the `sepmdd` utility in the *Reference Guide* and the `start_transaction` command in the *selang Reference section*.

## Use the seagent and sepmdd Daemons

The seagent daemon is responsible for accepting requests from remote computers and applying them to PMDBs; the seagent daemon also sends requests to seosd. The sepmdd daemon is the PMDB daemon. This section describes how these daemons work together in the PMDB environment.

**Use the table of contents to access the topics in this section.**

### The seagent Daemon

The seagent daemon waits for connections on the seoslang2 TCP service (whose default value is 8891). When a connection request arrives, seagent forks a child process to handle the communication on the connection and then continues waiting for new connections.

When a user enters the `hosts` command in `selang`, seagent forks a child process on the machine that the user is connected to. The child process then receives commands from the command language interface and passes them on to the sepmdd daemon.

### The sepmdd Daemon

The sepmdd daemon performs the following functions:

- Administers the PMDB
- Administers the subscriber databases
- Propagates changes from the PMDB to the subscriber databases

The sepmdd daemon is automatically started by seagent when seagent has to access the PMDB. Normally you do not need to run sepmdd explicitly.

**NOTE**

sepmdd runs under the logical user `_seagent` (*not* under root) in the AC environment. To permit or restrict access to resources by sepmdd (for example, to restrict access to the PMDB directory), create the relevant rules for `_seagent`.

## Use a Shadow File

Usually, sepmdd does not use a shadow file when updating a native environment. You can, however, set up a shadow file. To do this, set the UseShadow token in the [pmd] section of the pmd.ini file to yes.

If the UseShadow token is set to yes, sepmdd uses a default shadow file in the same directory as the PMDB. If you want to change the location of the shadow file, specify the new location with the YpServerSecure token in the [pmd] section of the pmd.ini.

If you change the location of the shadow file (with the YpServerSecure), to the local host's shadow file (for example, /etc/shadow), sepmdd sets a token, UseSystemFiles, to yes.

**WARNING**

Do not change the UseSystemFiles token yourself. The sepmdd or seagent daemons change it automatically.

**NOTE**

For more information about the seagent or sepmdd daemons, see the seagent and sepmdd utilities in the *Reference Guide*.

## Protect Idle Stations

Information is extremely vulnerable when terminals are left open and active. An intruder who happens upon such a terminal (for example, during a lunch break) need not try to break passwords or have complicated equipment to sniff the network lines, since all terminals at the site are already logged in and ready for work. Although screen savers that prompt for the password before restoring the desktop are useful, the security administrator cannot make sure that all users are using secured screen savers.

Privileged Access Manager provides selock, a screen-locking utility that guards all terminals and stations by locking them whenever they are idle for more than a specified period of time. When returning to work, the user is prompted to specify the password. If the correct password is not specified within one minute, the terminal remains locked. The selock utility can find the password of users who can unlock a screen even if those users change their passwords while selock is active.

**NOTE**

For more information about the screen lock utility selock, see the *Reference Guide*.

You should choose to use selock options that suit your requirements:

- Less security, more convenience  
Use the -timeout option to set the timeout to a large value, such as 10 minutes, and the -lock-timeout option to set the lock timeout to an even larger value, such as 60 minutes. This prevents selock from excessively interrupting your work by switching to the *saver* mode. Also, this setting locks your screen only in cases when your terminal is left inactive for extended periods.
- More security, less convenience

Use the `-timeout` option to set the timeout to a small value, such as 1 minute, and `-lock-timeout` option to set the lock timeout to a small value, between 0 and 2 minutes. This always hides your work soon after you stop accessing your terminal, and requires a password for restoring access. To ensure that `selock` always requires password-entry to reactivate your terminal after the saver mode starts, use the `-lock-timeout` option to set the lock timeout to zero.

- The `selock` command can be part of the X startup shell, so that it starts automatically every time the user logs in to the system. The script must be run under the user ID, not under the root ID. The way you integrate the `selock` command into the startup script depends on the specific environment of the site.

#### NOTE

For more information on startup scripts, see the documentation for your UNIX system.

## Choose a Protection Mode

`selock` offers three modes of operation:

- **Monitor Mode**

The monitor mode is the initial mode of `selock`. In this mode, `selock` monitors keyboard and mouse activity. If `selock` detects no keyboard or mouse activity during the time-out period--and the transparent parameter is off--`selock` automatically switches to the saver mode. No password entry is required for the transition from the monitor mode to the saver mode.

- **Saver Mode**

In the saver mode `selock` blanks the entire screen and displays a system icon that shifts position. The blank screen and shifting icon provide two operational advantages:

- Reduced risk of screen viewing by unauthorized people
- Reduced screen burn-in

You can manipulate the appearance and repositioning of the icon using `selock` options. When `selock` detects any keyboard or mouse activity, it immediately returns from the saver mode to the monitor mode, restoring the screen display to what it was before it switched to saver mode. No password entry is required for the transition from the monitor mode to the saver mode.

If `selock` remains in the saver mode for the period specified by the `lock-timeout` parameter, it automatically switches to the lock mode. `selock` does not give any visual indication of the transition from the saver mode to the lock mode.

- **Lock Mode**

In lock mode with the default settings, `selock` continues to display a moving icon on a black background. When `selock` detects any keyboard or mouse activity, a dialog containing a prompt for the user's password appears.

When the user enters the correct password, `selock` switches back to monitor mode. If the user enters an incorrect password, the password-entry dialog closes and `selock` remains in the lock mode.

If you set the `-transparent` option to `on`, `selock` locks the screen but displays the contents and updates the on-going processes. The background of the screen changes to indicate that the screen is locked. When you use the lock mode, saver mode is never invoked.

## Set Stations to Lock When Idle

The `selock` utility lets you lock idle stations to prevent unauthorized access to these stations when they are left idle.

### To set stations to lock when idle

1. (Optional) Set the `DISPLAY` environment variable.

#### NOTE

For the `selock` command to work, you must set the `DISPLAY` environment variable. However, you can specify the target display directly in the `selock` command instead.

2. Place the `selock` command in the user's login script (the `.login` file).  
Alternatively, you can place the `selock` command in the `/etc/login` or `/etc/cshrc` file.

**NOTE**

Two users can always unlock a locked screen. By default, these users are the current user and root. However, you can replace root with any other user if you specify the other user's name in the `unlocking_user` token, located in the `[selock]` section of the `seos.ini` file. You can replace the current user with any other user by using the `-user` option when executing `selock`.

**Example: Idle station lockup command in a startup file**

The following is a typical startup command, suitable to be placed in X startup files:

```
selock -display $DISPLAY -timeout 5
```

This command activates `selock` after five minutes of terminal inactivity.

We recommend that you place the following line in the global `xstartup` script. The `xstartup` script usually resides in the directory `/usr/lib/X11/xdm/Xstartup`.

```
selock -display $DISPLAY -user $USER -timeout 3 &
```

This statement enforces use of the terminal locking program for all users who are using X terminals.

**Change the Screen Lock Icon**

The default system icon that `selock` uses is the Privileged Access Manager logo and is located in the file `ACInstallDir/data/admin/Selogo.xpm`

To select an icon of your own choice, replace this file.

**NOTE**

The icon file must be in XPM version 3.3 format.

**Protect Resources Using APIs**

If you have defined resources that are not part of Privileged Access Manager (that is, in-house resources), you can protect them by using Privileged Access Manager APIs. Each API has two layers:

- **The function library**  
Enables programmers to use the Privileged Access Manager authorization engine.
- **The user exits**  
Enable the system administrator to tailor Privileged Access Manager behavior to the requirements of the site.

**NOTE**

For more information about Privileged Access Manager APIs, see the *SDK Guide*.

**Protect Against Stack Overflow STOP**

Stack overflow enables hackers to execute arbitrary commands on remote or local systems, many times as the root user (the superuser). They do this by exploiting bugs in the operating system or other programs. These bugs allow users to overwrite the program stack, changing the next command to be executed.

Stack overflow is not simply a bug; it is possible to create a block that overwrites the return address with a meaningful address, resulting in transferred control to unauthorized code (usually in the same block).

Stack Overflow Protection (STOP) is a feature that prevents hackers from creating and exploiting stack overflow to break into systems.



## Stack Overflow Protection on UNIX Linux Platforms

When using Stack Overflow Protection on a UNIX or Linux platform, consider the following:

- (Solaris 11 AMD) STOP is disabled for Solaris 11 and later because Solaris 11 natively provides stack protection: Solaris 11 changes process stack location and has built-in support for Address Space Layout Randomization (ASLR). By default, this protection is turned on for tagged files, which includes zones.
- (Red Hat Linux, SuSE Linux) When Linux native stack randomization (exec-shield-randomize) is enforced, the STOP feature is not activated.

To deactivate native stack randomization, enter the following command:

```
echo 0 > /proc/sys/kernel/exec-shield-randomize
```

## Start and Stop STOP

When STOP is first installed, stack overflow protection is activated by default. To deactivate it, you must change a token in the [seos\_syscall] section of the seos.ini file and restart Privileged Access Manager. To do this, use the seini command as follows:

```
seini -s SEOS_syscall.STOP_enabled 0
```

You could manually change the seos.ini file instead.

To re-enable STOP, change the value of the token to 1 and restart Privileged Access Manager.

### NOTE

When STOP is active on Sun Solaris 7 systems, the dbx program cannot work properly. If you need to use dbx on a system that is protected by STOP, you must first disable STOP.

## Define Day and Time Access Rules for Resources

You can use Privileged Access Manager to specify day-of-week and time-of-day restrictions for resource access. This feature can be exploited for TERMINAL access, SURROGATE requests, and user-defined resources. For example, the following rule completely disables the terminal ws3 on weekends and outside the 08:00-19:00 time period every day:

```
chres TERMINAL ws3 restrictions(days(weekdays) time(0800:1900))
```

No login request from that station is accepted outside these periods.

You can use Privileged Access Manager to protect against substitution requests to highly authorized users outside work hours. Suppose user AcctMgr is the Accounting Manager, who is allowed to perform financial transactions, and you have restricted AcctMgr login to work hours and weekdays only. Intruders or unauthorized personnel may try to access the account of AcctMgr by invoking the command **su** AcctMgr. Use the following command to make it impossible to substitute the user name to AcctMgr outside the specified period:

```
chres SURROGATE USER.AcctMgr restrictions(days(weekdays) time(0800:1900))
```

The same technique can be implemented for any protected resource, including user-defined abstract classes that are used for implementing in-house applications.

## Protect System Devices

You can use Privileged Access Manager to protect system devices against unauthorized copy. By creating a copy of an existing system node, unauthorized accessors can export the content of the protected device and read the content as raw data.

When a user attempts to create a block-oriented or character special file based on an existing one using the `mknod` command, Privileged Access Manager checks the device. If the user attempts to create a copy of a protected device, Privileged Access Manager blocks the attempt and prevents the operation.

By default, Privileged Access Manager does not block the device copy operation.

You can enable the system devices protection from the `seos.ini` file under the `SEOS_syscall` section in the `file_rdevice_max` token.

#### NOTE

For more information about the `file_rdevice_max` token, refer to the *Reference Guide*.

## Security Levels (UNIX)

When security level checking is enabled, Privileged Access Manager performs security level checking in addition to its other authorization checking. A security level is a positive integer from 1 through 255 that can be assigned to users and resources. When a user requests access to a resource that has a security level that is assigned to it, Privileged Access Manager compares the security level of the resource with the security level of the user. If the security level of the user is equal to or greater than the security level of the resource, Privileged Access Manager continues with other authorization checking. Otherwise, the user is denied access to the resource.

If the `SECLABEL` class is active, Privileged Access Manager uses the security level associated with the security labels of the resource and user; the security level that is explicitly set in the resource and user records is ignored.

- To protect a resource with security level checking, assign a security level to the record of the resource. The `level` parameter of the `newres` or `chres` command assigns a security level to a resource.
- To allow a user access to resources protected by security level checking, assign a security level to the record of the user. The `level` parameter of the `newusr` or `chusr` command assigns a security level to a user.

## Enable Security Level Checking

The following `setoptions` command enables security level checking:

```
setoptions class+ (SECLEVEL)
```

## Disable Security Level Checking

The following `setoptions` command disables security level checking:

```
setoptions class- (SECLEVEL)
```

## Security Categories (UNIX)

When security category checking is enabled, Privileged Access Manager performs security category checking in addition to its other authorization checking. When a user requests access to a resource that has one or more security categories assigned to it, Privileged Access Manager compares the list of security categories in the resource record with the category list in the user record. If every category assigned to the resource appears in the category list of the user, Privileged Access Manager continues with other authorization checking; otherwise, the user is denied access to the resource.

If the `SECLABEL` class is active, Privileged Access Manager uses the list of security categories that are associated with the security labels of the resource and user; the lists of categories in the user and resource records are ignored.

To protect a resource by security category checking, assign one or more security categories to the record of the user. The `category` parameter of the `newres` or `chres` command assigns security categories to a resource.

To allow a user access to resources protected by security category checking, assign one or more security categories to the record of the user. The category parameter of the `newusr` or `chusr` command assigns security categories to a user.

## Enabling Security Category Checking

The following `setoptions` command enables security category checking:

```
setoptions class+ (CATEGORY)
```

## Disable Security Category Checking

The following `setoptions` command disables security category checking:

```
setoptions class-(CATEGORY)
```

## Define a Security Category

Define a security category by defining a resource in the `CATEGORY` class. The following `newres` command defines a security category:

```
newres CATEGORY name
```

where *name* is the name of the security category.

To define the security category *Sales*, enter the following command:

```
newres CATEGORY Sales
```

To define the security categories *Sales* and *Accounts*, enter the following command:

```
newres CATEGORY (Sales,Accounts)
```

## List Security Categories

To display a list of all the security categories that are defined in the database, use the `show` command as follows:

```
find CATEGORY
```

The list of security categories displays on the screen.

## Delete a Security Category

Delete a security category by removing its record from the `CATEGORY` class. The following `rmres` command removes a security category:

```
rmres CATEGORY name
```

where *name* is the name of the security category.

To remove the security category *Sales*, enter the following command:

```
rmres CATEGORY Sales
```

## Security Labels (UNIX)

A security label represents an association between a particular security level and zero or more security categories.

When security label checking is enabled, Privileged Access Manager performs security label checking in addition to other authorization checks. When a user requests access to a resource that has a security label that is assigned to it, Privileged Access Manager makes the following comparison: the product compares the list of security categories specified in the resource record's security label with the list of security categories specified in the user record's security label. If every category assigned to the resource's security label appears in the user's security label, Privileged Access Manager continues with the security level check. Otherwise, the user is denied access to the resource. Privileged Access Manager compares the security level specified in the resource record's security label with the security level specified in the user record's security label. If the security level assigned in the user's security label is equal to or greater than the security level assigned in the resource's security label, Privileged Access Manager continues with other authorization checking; otherwise, the user is denied access to the resource.

When security label checking is enabled, the security categories and security level specified in the user and resource records are ignored; only the security level and categories that are specified in the security label definitions are used.

To protect a resource by security label checking, assign a security label to the resource's record. The label parameter of the newres or chres command assigns a security label to a resource.

To allow a user access to resources protected by security label checking, assign a security label to the record of the user. The label parameter of the newusr or chusr command assigns security labels to a user.

## Enable Security Label Checking

The following setoptions command enables security label checking:

```
setoptions class+(SECLABEL)
```

## Disable Security Label Checking

The following setoptions command disables security label checking:

```
setoptions class-(SECLABEL)
```

## Define a Security Label

Define a security label by defining a resource in the SECLABEL class. The following newres command defines a security label:

```
newres SECLABEL name category(securityCategories) level(securityLevel)
```

where:

- **name**  
Specifies the name of the security label.
- **securityCategories**  
Specifies the list of security categories. To specify more than one, separate the security category names with a space or a comma.
- **securityLevel**  
Specifies the security level. Use an integer between 1 and 255.

To define the security label Managers to contain the security categories Sales and Accounts and a security level of 95, enter the following command:

```
newres SECLABEL Manager category(Sales,Accounts) level(95)
```

## List the Security Labels

To display a list of all the security labels that are defined in the database, use the show command as follows:

```
find SECLABEL
```

The list of security labels appears on the screen.

## Delete a Security Label

A security label is deleted by removing its record from the SECLABEL class. The following rmres command removes a security label:

```
rmres SECLABEL name
```

where *name* is the name of the security label.

To remove the security category, *Manager* enter the following command:

```
rmres SECLABEL Manager
```

## Audit Logs (UNIX)

The audit records are stored in a file that is named the audit log. The location for the audit log is specified in the seos.ini file. Use the seaudit utility or Privileged Access Manager Endpoint Management to list recorded events in the audit log. Filter events by time restrictions or event type, and so on.

### NOTE

For more information about seaudit, see the *Reference Guide*.

The audit logs are stored locally. However, you can use Privileged Access Manager to distribute the auditing information by using the log routing facility. Consider archiving old audit logs to tape, to allow you to scan the events later.

By default, the authorization daemon seosd creates the audit logs with root ownership, because the user root executes the seosd program. For the same reason, the audit logs are created with read/write permissions granted only to root.

To enable other users to read the audit logs without having to su (substitute user) to root, Privileged Access Manager includes two entries in the seos.ini file. These entries specify which group ownership is assigned to the log files.

- One entry is for the audit log.  
Suppose that the auditors at your site are all members of a group named auditforce. You want these users to be able to browse through the local audit log files. Edit the seos.ini file so that the audit\_group token in the [logmgr] section is set to auditforce. Privileged Access Manager then gives the auditforce group read permission to your local audit logs. From this point, any local audit logs created at your station have the auditforce group as their owner.  
The log routing daemons consult the same token to see who can have access rights to the audit logs that the daemons produce and collect. The audit logs are subject to access control like any other files, and Privileged Access Manager rules can keep users from accessing them.
- The other entry is for the error log. This entry is used in the same way to specify group ownership for that file.

## Configure an Endpoint to Send seaudit Logs to syslog

This article explains the procedure to configure Privileged Access Manager endpoint to send *seos* audit logs to *syslog*. This procedure is helpful when a syslog collector is installed on an endpoint and you must collect endpoint *seos* audit logs along with syslogs.

**Follow these steps:**

1. Stop the Privileged Access Manager endpoint agent.  
`<INSTALL_DIRECTORY>/PAMSC/bin/secons -sk`  
`<INSTALL_DIRECTORY>` is the directory where the Privileged Access Manager endpoint agent is installed.
2. Open `<INSTALL_DIRECTORY>/PAMSC/log/selogrd.cfg` for editing (if it does not exist, create the file). Add the following rule to the file:

```
Rule#1
syslog LOG_INFO
.
```

**Note:** '.' at the end of the rule is mandatory.

3. Save the file.
4. Restart the Privileged Access Manager endpoint agent.  
`<INSTALL_DIRECTORY>/PAMSC/bin/seload`
5. Restart the `selogrd` daemon.  
`<INSTALL_DIRECTORY>/PAMSC/bin/selogrd`
6. Restart `syslogd` on the server.

Now you can view the `seos` audit logs in the messages file (`/var/log/messages`).

**Detect and Handle Failed Logins through SSH**

To prevent brute force-based break-in attacks into UNIX systems, Privileged Access Manager for UNIX provides detection of the failed user logons on a host and revocation of the user ID.

The `serevu` module facilitates revocation and optional subsequent re-enablement of a revoked user ID.

This topic describes how to configure Privileged Access Manager to detect and handle failed logins that occurred on SSH. This topic also helps you understand the data flow between failed logins through SSH, PAM (Pluggable Authentication Modules), `seosd`, and `serevu`.

**Follow these steps:**

1. Configure the `serevu` module to detect failed logins occurred through applications that use PAM. PAM is the default authentication subsystem on UNIX-flavors.  
 To allow `serevu` to work with PAM, set the following token in the `seos.ini` configuration file:

```
[pam_seos]
serevu_use_pam_seos = yes
```

2. To configure `sshd` to use PAM for authentication, set the following token in `/etc/opt/ssh/sshd_config`:  
`UsePAM yes`

This configuration allows the daemon `sshd` to signal the PAM system that a failed login occurred.

3. Add the following line to `/etc/pam.conf` to ensure Privileged Access Manager is set up to intercept PAM signals coming from `sshd`:

```
sshd auth optional /usr/lib/security/pam_seos.sl
```

4. Ensure that the local `seosdb` holds a `loginappl` record for the `sshd`. Add the following lines in `Selang`:

```
PAMSC> nr loginappl SSHD loginpath(/usr/sbin/sshd) loginseq(SGRP SUID) defaccess(x)
```

You can now find any failed logins done on an SSH client in the file: `/opt/CA/PAMSC/log/pam_seos_failed_logins.log`

With this configuration done, the data flows as follows:

- a. `sshd` signals PAM that a failed login occurred.
  - b. Privileged Access Manager intercepts this PAM signal and writes information into the `pam_seos_failed_logins.log`.
  - c. `serevu` periodically scans that log and acts accordingly.
5. The number of failed logins each user is entitled to before being revoked can be set in `seos.ini`.

```
[serevu]
def_fail_count = 3
```

6. To startup `serevu` automatically upon `seload`, add the following code to `seos.ini`:

```
[daemons]<>
serevu = yes
```

## The System Auditor

A system auditor is a user to whom the AUDITOR attribute is assigned. Users defined as system auditors are permitted to perform auditing tasks such as changing the auditing attribute that is assigned to users and resources.

Auditing tasks can be carried out from central locations. To collect auditing information from the various stations on the network in a single host, the auditor can use the log routing facility.

## Set Up the Log Routing Facility

### To set up the log routing:

1. Create a log routing configuration file.  
Unless you specify otherwise with the `RouteFile` token in the `seos.ini` file, Privileged Access Manager expects your log routing configuration file to be named `ACInstallDir/log/selogrd.cfg` where `ACInstallDir` is the installation directory for Privileged Access Manager, by default `/opt/CA/PAMSC`. You can find sample log routing configuration files in the directory `ACInstallDir/samples/selogrd.init`. Alternatively, as a very simple log routing configuration file, you can create a file consisting of the following three lines:

```
Rule
host destination
.
```

For *destination*, enter the name of the host that should receive the audit records. All classes, resources, accessors, and results are logged.

#### NOTE

For more information about the syntax of the configuration file, see the `selogrd` utility in the *Utilities section*.

2. Start the emitter daemon (`selogrd`) on all hosts that are to route auditing information, and execute the collector daemon (`selogrcd`) on all hosts that are to collect auditing information.

#### NOTE

For more information about using these daemons, see the *Reference section*.

## File Notifications

In addition to compiling the log, the log routing facility can send notifications to the display screen of the host, to an email address, or to other destinations. You can base notifications on information from your station's own audit log or from logs that the collector daemon has brought to your station.

To set up such notifications, use the log routing configuration file *and* a selang command. Example: Notify the user John whenever a setuid request to the user root is successfully made.

1. Issue the following selang command:

```
chres SURROGATE USER.root notify(John)
```

This chres command specifies that each time someone surrogates user to root, a special audit log record is created, and the seosd daemon is to notify the user named John. The daemon also creates a special audit record that is named a *notification record*.

2. Once you have specified notification for one or more resources, you can add the following three lines to the log routing configuration file.

```
Rule2
notify default
.
```

This line causes the log routing emitter to create a mail message for the notification audit record.

### NOTE

For more information about the configuration file format and setting up the log routing daemons, see the *Reference Guide*.

## Log Routing

Privileged Access Manager uses the log routing daemon, selogrd, for the following tasks:

- To distribute selected local audit log records to specific hosts
- To reformat audit log records in to email messages, ASCII files, or user windows
- To transmit notification messages based on audited events

To determine audit record routing, selogrd uses a configuration file, selogrd.cfg. This file is a list of which audit log records to route, or not to route, and where to route them. For a complete description of this file, see the *Reference Guide*.

**Use the table of contents to access the topics in this section.**

## Log Routing Configuration

To start selogrd or selogrcd automatically when seosd starts, set the seos.ini tokens selogrd or selogrcd in the [daemons] sections to yes. Then when you run seload, seload starts the daemons for you.

For example, the appropriate tokens in the [daemons] section of the soes.ini should look as follows:

```
selogrd = yes
selogrcd = yes
```

Since the log-routing facility uses RPC to route audit records, placing a log audit collector behind a firewall does not allow simple blocking of UDP ports because there is no way to know which port the portmapper assigns to the server daemon. To solve this problem, you can use the token ServicePort to assign a predefined port to the server daemon.

If the firewall allows port 111 from outside the network (portmapper port), you should only change the seos.ini file in the server. If the firewall does not allow communication to portmapper in the protected network, both clients and server must agree on a specific port.



You can ensure this by setting the same value in the ServicePort token in the seos.ini files of both clients and the server. You can specify a number--which means that the daemons bind to the specified port--or a service name. If you specify a service name, both clients and the server must have the same service resolution. For example, if you specify the service name seoslogr, then add the following to the /etc/services file of the clients and the server:

```
seoslogr 2022/udp # Audit log-routing
```

If the clients or the server are using NIS to resolve services, you must update the NIS services map.

## Audit Log Route Encryption

You can encrypt audit log records. When you use encryption, the selogrd daemon encrypts audit log record before sending it to the collector (selogrcd or audit log router). The collector in turn decrypts the received records.

Privileged Access Manager provides two encryption styles for selogrd: Privileged Access Manager standard encryption, and audit log encryption through adcipher. For encryption, selogrd uses functions from shared library objects, as specified in the [selogrd] section of the seos.ini file.

Standard encryption uses the shared library libcrypt; Audit encryption uses functions from a file specified by the CipherName token. By default, the file name is adcipher, which is a symbolic link to the desired shared library. The product installation process places four shared libraries in the lib directory: lib1des, lib3des, libIDEA, and libblowfish.

Privileged Access Manager maintains the standard encryption key in the shared library, while the audit encryption uses a separate file as specified by the KeyFile token (default value: adcipher.bin).

Use the UseEncryption token to determine the type of encryption:

- To use Privileged Access Manager standard encryption, specify UseEncryption=native.
- To use audit log encryption through adcipher, specify UseEncryption=eTrust, and enter the appropriate values for the CipherName and KeyFile tokens.
- To disable selogrd encryption, specify UseEncryption=no.

Use the RefuseUnencrypted token to accept or deny unencrypted audit. It is used in conjunction with the UseEncryption token and is redundant if the UseEncryption is set to no:

- To refuse unencrypted audit, specify RefuseUnencrypted=yes
- To accept both encrypted and unencrypted audit, specify RefuseUnencrypted=no

**Note:** The selogrcd daemon uses the same tokens in the seos.ini file.

To change the encryption key, use the seckey utility, described in this chapter.

### WARNING

If you send records to the audit collector, be sure that both selogrd and the collector use the same shared encryption file and encryption key.

## Send Audit Log Records using Email

selogrd can send records to email targets directly. You can direct email messages through a mailer utility, or directly to the mail exchange server using SMTP.

To send audit log records directly to the mail exchange server, set the UseSmtpMail token in the [selogrd] section of the seos.ini file.

You can specify the following:

- A time-out in case the mail server does not answer, using the `SmtptimeLimit` token
- The From: mail header field, using the `SmtptimeFrom` token
- The mail server host address, using the `SmtptimeServer` token

**NOTE**

This method does not use UNIX mail utility; rather, it establishes a direct connection with mail server, and uses SMTP protocol to send mail.

**Configure SNMP Traps**

For systems that use the Internet network management protocol SNMP (Simple Network Management Protocol), you can configure `selogrd` to create SNMP traps using Privileged Access Manager audit records.

To implement the SNMP traps, first locate the SNMP shared objects provided in the Privileged Access Manager libraries, and then configure `selogrd` correctly using these shared objects.

**Note:** If you want to use the SNMP extension of `selogrd`, and Privileged Access Manager is not installed in the default location (`/opt/CA/PAMSC`), set an environment variable before running `selogrd`. The environment variables are as follows, where *ACInstallDir* is the directory where you installed Privileged Access Manager:

- In AIX, set `LIBPATH` to *ACInstallDir*/lib
- In Solaris, set `LD_LIBRARY_PATH` to *ACInstallDir*/lib
- In LINUX, set `LD_LIBRARY_PATH` to *ACInstallDir*/lib
- In HP, set `SHLIB_PATH` to *ACInstallDir*/lib

The shared objects-usually found in the directory *ACInstallDir*/lib- are called `snmp.xx` and `libsnp.xx`, where the `xx` extension varies according to the platform. The possible extensions are:

- `.o` AIX platform
- `.sl` HP platform
- `.so` All other platforms

If you want to use the SNMP extension of `selogrd`, and Privileged Access Manager is not installed in the default location, you must set the following environment variables before running `selogrd`:

- In AIX, set `LIBPATH` to *ACInstallDir*/lib
- In Solaris, set `LD_LIBRARY_PATH` to *ACInstallDir*/lib
- In Linux, set `LD_LIBRARY_PATH` to *ACInstallDir*/lib
- In HP, set `SHLIB_PATH` to *ACInstallDir*/lib

where *ACInstallDir* is the directory where you installed Privileged Access Manager.

**Follow these steps:**

1. Create a file called *ACInstallDir*/etc/`selogrd.ext`.
2. Define where the SNMP shared objects are by adding a single line to the file *ACInstallDir*/etc/`selogrd.ext` with the appropriate path for the `snmp.so`. (It is enough to specify this shared object for the other to automatically be linked.) For example:

```
snmp /opt/CA/PAMSC/lib/snp.so
```

3. Finally, you must configure the `selogrd.cfg` file to specify what type of action should trigger SNMP traps, and which location should be notified when SNMP traps are triggered. Configuration is very similar to that for other auditing notification, with the delivery system specified as `snmp`.

For example, suppose you want to have SNMP traps activated when Privileged Access Manager starts and shuts down, and have notification of these SNMP traps sent to AuditPC. You can do this by adding the following section to the `selogrd.cfg` configuration file:

```
snmpRule

snmp AuditPC

include Class(START) .

include Class(SHUTDOWN) .

.
```

To send SNMP traps to a gateway with a community name, use the following format:

```
snmp gateway[@community name]
```

#### Example:

```
snmp AuditPC@secure
```

Similarly, you can activate the SNMP traps by other actions or types of access, or have them sent to other locations.

## Migrate User Trace Filters

If you set a user to be traceable, each time a trace record is written for that user, a matching audit record is written to the `seos.audit` file. In previous releases of Privileged Access Manager, these audit records were filtered by the `trcfilter.init` file. In Privileged Access Manager r12.0 SP1 and later, the audit records generated by user trace records are filtered by the `audit.cfg` file, which filters all other audit records.

You must manually migrate the audit record filters from `trcfilter.init` to `audit.cfg`. If you do not migrate the filters, the audit records generated by user traces will not be filtered.

#### NOTE

Trace records are still filtered by `trcfilter.init`. Do not migrate trace filters from `trcfilter.init` to `audit.cfg`.

#### Follow these steps:

1. In `trcfilter.init`, find the user trace filter that you need to migrate.  
The `trace_filter` setting in the `seosd` section of the `seos.ini` file determines the location of this file.
2. In `audit.cfg`, type the following, where *usertracefilter* is the user trace filter from `trcfilter.init`:  
`TRACE;*;*;*;usertracefilter`
3. (Optional) Repeat Steps 1-2 for each user trace filter that you need to migrate.

#### Example: Migrate User Trace Filter

In this example, the following user trace filter is in the `trcfilter.init` file:

```
*ExampleFilter
```

To migrate this user trace filter, type the following on a new line in the `audit.cfg` file:

```
TRACE;*;*;*;*ExampleFilter
```

## Improve Performance

This section describes different ways to improve performance on UNIX endpoints.

### Use Global Access Check

The Global Access Check feature (GAC) lets you access protected, frequently opened files--whose access rules are unlikely to change--much faster than otherwise possible.

GAC allows a Privileged Access Manager administrator to cache rules for read, write, chown, chmod, rename, unlink, utimes, chattr, link, chdir, create, and all, so that appropriate access to files is granted without passing control to seosd. The default is all. Execute requests, however, are not eligible for GAC because they could pose a security loophole.

Without GAC, Privileged Access Manager runs thorough security checks whenever a user or program attempts to access protected files. Frequently accessed files need repeated in-depth checks to confirm access permissions.

GAC allows an administrator for Privileged Access Manager to take for granted that certain frequently accessed protected files require shorter security checks. An administrator for Privileged Access Manager can select files suitable for a shorter check. Before Privileged Access Manager allows a shorter security check, the file must first undergo a full security check based on the set rule. The rule itself consists of a generic file name and a list of accesses. Rules are cached according to users.

Selecting certain files for a shorter check is reliable because, with the GAC feature in place, if a change is actually made to rules regarding the protected files, the shorter security check table is flushed, and an initial full security check is instituted.

#### NOTE

GAC restrictions mean that this feature works for every user except root.

### How Does Global Access Check Work

Privileged Access Manager monitors access to specified files and builds a table of permitted accesses during execution time. These are the files you specify in advance in order to set up Global Access Check (GAC) rules.

Whenever Privileged Access Manager concludes that a user should be granted a certain level of access to a certain file, it checks whether the following two additional conditions are met:

- The granted access is unconditional. It is not dependent on time, day, program from which executed, or other conditions.
- The file matches one of its preselected sets of file masks.

#### NOTE

File rules define permissions for access to files.

#### NOTE

If these conditions are met, Privileged Access Manager generates a UID-file rule-access triplet and stores it in a table composed of such triplets. This table is examined before any database access rule interpretation takes place. Whenever a user attempts to access a file, this table is consulted as a filtering mechanism.

The table is best described as a do-not-call-me table because it contains a list of file masks that, once recognized, no longer need to undergo access permission checks. It is also described as an always-grant table because access is always granted to files specified within its list of file masks.

Whenever a user attempts to access a file, the table is consulted. If the file matches one of the triplets found in the table, the appropriate access is granted without passing control to seosd. This bypasses the access rules analysis. Subsequently, all access to files that match this pattern is granted, based on the triplet stored in the table, without consulting the access rule database.

Whenever a new access rule is added to the database, the entire table is flushed, and the learning process starts from the beginning.

## Implement Global Access Check

To set up Global Access Check (GAC), choose masks for sets of files that are accessed often, set up a GAC file containing these file masks, and then start the caching process.

### Set Up Global Access Check Rules

#### NOTE

File rules in the database are created using the class FILE parameter and file masks. Rules apply to all files matching the file masks. FILE access types include: all, chdir, control, create, delete, execute, none, read, rename, sec, update, utime, write.

From the file rules defined in the database, choose the file masks that you want to cache. Enter a list of file masks into the *ACInstallDir/etc/GAC.init* file (where *ACInstallDir* is the installation directory for Privileged Access Manager, by default /opt/CA/PAMSC), in exactly the same form as they appear in the database.

Each such mask should be specified on a separate line. For example, if the database contains a file mask for */tmp/mydir/\** and you want it to be cached, add the following line to the *ACInstallDir/etc/GAC.init* file:

```
/tmp/mydir/*
```

#### NOTE

Specific file names cannot be specified in the GAC.init file. Only file masks are used.

### Start Global Access Check

To turn your current version of Privileged Access Manager into a Global Access Check (GAC)-compatible version, prepare the file *ACInstallDir/etc/GAC.init* with the file masks that are eligible for caching. Only file masks can be used.

An example is a file named GAC.init in *ACInstallDir/etc/* with only one line:

```
/IBBS/REL63/*
```

## Use the Resource Cache

Another performance improvement tool that Privileged Access Manager offers is resource caching (file cache).

The cache remembers the previous answer to an authorization request (permit or deny) for resources in the FILE class. The result is saved with the file name, user name, and authorization response (access mode, program name, and result). When an identical authorization is requested, the request is answered with the last response that was stored in the cache memory tables. This saves time because Privileged Access Manager does not have to reevaluate the request; Privileged Access Manager can return the answer immediately. When rules are changed, the cache is automatically and immediately synchronized.

The cache is a runtime table. An administrator can configure it in two ways:

- Set initialization parameters in the seos.ini file.
- Switch caching to ON or OFF and change parameters at runtime.

The security administrator can define table size, intervals between cleaning tables, and other internal table parameters with tokens in the seos.ini file.

A user with administrative privileges can switch cache tables ON or OFF, change cache parameters, and write cache tables to standard output.

**NOTE**

For more information about the secons utility or the [seosd] section of the seos.ini initialization file, see the *Reference Guide*.

## Tuning Recommendations

Use these recommendations to improve performance even more:

- If one of the three tables (pools) has the maximum number of records and another table does not, expand the size of the full table.

**NOTE**

The three tables are file, user, and authorization. If a pool has low settings, increase them to expand the pool.

- Do not set the maximum size tokens unless you must. Larger tables take more time when scanning for records.

## Use the Network Cache

The network or IP caching feature stores accepted, incoming TCP requests, so they are not sent to the database. Instead, they are automatically permitted with the syscall function. This feature improves performance for hosts, which launch many incoming TCP connections.

To activate the IP caching feature, change the following tokens in the [seosd] section of the seos.ini file and restart Privileged Access Manager:

- **network\_cache\_timeout**  
Defines how often to clean the cache table. This token is important if you want to set time limits for the accept requests.
- **UseNetworkCache**  
Set this token to yes to activate IP caching.

When caching is enabled, all accepted TCP connections are saved in the kernel table. The records consist of a peer IP address, peer port, and local port. Every new connection is searched in this cache. If a matching set of data for IP address, IP port, and local port is located, the connection is immediately permitted. The time to establish connection is reduced.

## Use the Real Path Cache

File name resolution is a long process because Privileged Access Manager uses information from the file system. The kernel of Privileged Access Manager translates node numbers to full file names when it intercepts appropriate events. Real path caching saves file names within an internal table.

To enable this feature, set the token cache\_enabled to 1 in the [SEOS\_syscall] section of the seos.ini file. File names are cached in the table with a data pair: inode number and device number.

**NOTE**

For more information about the seos.ini initialization file, see the *Reference Guide*.

## Use Fork Synchronization

The fork synchronization token (synchronize\_fork) in the [SEOS\_syscall] section of the seos.ini file manages fork event behavior when new processes are created. Lowering the value of this token improves performance because fork events are frequent.

**NOTE**

For more information about seos.ini initialization file, see the *Reference Guide*.

**Use High Priority**

Privileged Access Manager contains an option to set a real-time priority for the seosd daemon on some platforms. To activate this feature, set the `rt_priority` token in the `[seosd]` section of the `seos.ini` file to `yes`. Running in real time improves system performance.

**NOTE**

For more information about the `seos.ini` initialization file, see the *Reference Guide*.

**Bypass the Process File System**

To reduce system load, you can specify whether Privileged Access Manager should check file access when the file belongs to a process file system (`/proc`).

To activate this feature, use the `proc_bypass` token in the `[SEOS_syscall]` section of the `seos.ini` file. The token stores access information to be bypassed whenever Privileged Access Manager must access the process file system.

**NOTE**

For more information about `seos.ini` file tokens, see the *Reference Guide*.

**Bypass Real Paths**

Searching for files with absolute file paths (instead of relative paths) creates heavier system loads; bypassing this search accelerates file events.

To activate this bypass, set the `bypass_realpath` token to `1` in the `[SEOS_syscall]` section of the `seos.ini` file. If you enable this token, Privileged Access Manager does not obtain real file names, which, for example, could be a symbolic link.

**NOTE**

For more information about `seos.ini` file tokens, see the *Reference Guide*.

**WARNING**

This feature should be used with extreme care because it impacts security-generic rules that do not work when files are accessed with a relative path.

**Bypass Trusted Process Authorization**

Privileged Access Manager allows you to define programs as trusted. Privileged Access Manager stores the trusted programs and their children programs in a table. All events (inbound *and* outbound) related to trusted processes (and their corresponding ports) are permitted without authorization as part of a full network bypass.

To specify these programs, use the `SPECIALPGM` class:

- To bypass file and network events for the specified program, use the property `PGMTYPE` with values `pbf` and `pbn`.
- To bypass `setuid` and `setgid` events for a specified program, use the property `PGMTYPE` with the value `surrogate`.
- To bypass all Privileged Access Manager authorization checks for a specified program, use the property `PGMTYPE` with the value `fullbypass`.  
Privileged Access Manager ignores a process that has the `PGMTYPE(fullbypass)` property, and no record of any process events appears in Privileged Access Manager audit, trace, or debug logs.
- To propagate bypasses to all programs that are called from the specified program, use the property `PGMTYPE` with the value `propagate`.

**NOTE**

Security privilege propagation works with PBF, PBN, DCM, FULLBYPASS, and SURROGATE privileges only.

**Bypass Ports for Network Activity**

To specify that all connection events (inbound *and* outbound) related to specific TCP/IP ports can be established without Privileged Access Manager authorization, you can define a bypass for these ports. Bypassing these ports reduces system load and speeds event processing. Bypassed connection events are not logged in the audit and trace files.

**NOTE**

Privileged Access Manager lets you bypass the network connection event only, not any subsequent events that use the network connection (for example, opening a file).

Trusted inbound connections are specified separately from outbound connections:

- To bypass *incoming* connections, modify the *bypass\_TCPIP* configuration setting in the [seosd] section of the seos.ini file.
- To bypass *outgoing* connections, modify the *bypass\_outgoing\_TCPIP* configuration setting in the [seosd] section of the seos.ini file.

**NOTE**

For more information about the seos.ini initialization file, updating tokens, and affecting changes, see the *Reference Guide*.

**Example: Bypass incoming Telnet events**

If you set the *bypass\_TCPIP* configuration setting to 23 (the Telnet port), the audit and trace files no longer log the network event when you Telnet *to* that workstation. Events related to other services, such as ssh, login, and FTP, and subsequent events that use the network connection (for example, opening a file), will still be logged.

**Example: Bypass outgoing FTP events**

If you set the *bypass\_outgoing\_TCPIP* configuration setting to 21 (the FTP port), the audit and trace files no longer log the network event when you FTP *from* that workstation. Events related to other services, such as ssh, login, and Telnet, and subsequent events that use the network connection (for example, opening a file), will still be logged.

**Reduce Audit and Trace Loads**

Privileged Access Manager uses a file system to keep audit data and trace data. Most processes in the system could be blocked while Privileged Access Manager writes to this file system. To reduce access time to the file system, do the following:

- Set the audit mode only for resources and accesses you need.
- Open the trace only when you need to.
- Store audit file, trace file, and Privileged Access Manager database files on the fastest available file system.
- Store the lookaside database directory on a fast file system.

**Reduce Database Loads**

How you define rules to the database effects system performance:

- Generic rules for commonly used directories produce many verifications, resulting in a greater system load. For example, protecting `/usr/lib/*` causes every action in the system to be checked by Privileged Access Manager. To improve performance, avoid using generic rules for frequently used files.
- Deep hierarchies of users and resources require system loads to obtain and check all dependencies. To improve performance, avoid deep hierarchies in the database.



## Improve PMDB Updates

Policy Models send commands to their subscribers one by one in a loop. To control the maximum number of commands that the Policy Models send to each subscriber during each loop, use the `updates_in_chunk` token, which is described in the [pmd] section of the appendix, "The pmd.ini File."

If you increase the value of this token, the Policy Model uses fewer cycles to send commands. After each loop, the Policy Model checks for new requests. If the token is set higher, the Policy Model does not check for new requests as often.

For example, when you add a new subscriber to the Policy Model (using the `sepm -n` option), increase the token value because other subscribers have already received the commands that the Policy Model is sending. The Policy Model spends less time sending commands to the other subscribers and spends more time sending commands to the new subscriber, shortening the time it takes to add the subscriber.

### NOTE

Do not set this token value to more than 100.

## Improve Watchdog Performance

To reduce system load, set the Watchdog daemon (`seoswd`) to periodically scan secured files instead of constantly scanning. You can specify the Watchdog to scan at times when the system is less loaded.

To activate this feature, use the `IgnoreScanInterval` token in the [seoswd] section of the `seos.ini` file, and set additional tokens for intervals and start times.

### NOTE

For more information about these tokens, see the `seos.ini` initialization file in the *Reference Guide*.

## Improve Class Parameters

Use the class activation and class authorization features for Privileged Access Manager to improve performance further.

### Class Activation (UNIX)

Privileged Access Manager stores information about whether a CLASS is active or inactive in the database. When Privileged Access Manager starts, it passes a list of active classes to `SEOS_syscall`, so Privileged Access Manager does not have to constantly intercept these classes. The only time Privileged Access Manager intercepts a class is when a user changes the activity status of a class. If a class is inactive, access to the resource is not intercepted.

You can use the inactive class bypass with the following classes: FILE, HOST, TCP, CONNECT, and PROCESS.

### Class Authorization

The resource class SEOS controls the behavior of the Privileged Access Manager authorization system. The SEOS class has modifiable properties that specify whether a class is active. You can disable unused classes (using the `setoptions` command) to reduce authorization time.

## Resolve Names

Several tokens in the [seosd] section of the `seos.ini` file (including `GroupidResolution`, `HostResolution`, `ServiceResolution`, and `UseridResolution`) control how Privileged Access Manager performs name resolution. Setting these tokens appropriately improves performance.

Alternatively, you can create a lookaside database (instead of using system name resolution). To improve performance, select the lookaside database option. Tokens for this feature include the `lookaside_path` and `use_lookaside`.

**NOTE**

For more information about these tokens, see the seos.ini initialization file in the *Reference Guide*.

Whenever Privileged Access Manager must perform UID to username, GID to groupname, ipaddr to host name, and port to service translations, it may have an impact on Privileged Access Manager performance. How Privileged Access Manager performs these translations depends on the value of certain tokens in the seos.ini file--in particular, the under\_NIS\_server, use\_lookaside, GroupidResolution, HostResolution, ServiceResolution, UseridResolution, and resolve\_timeout tokens.

When native operating system mechanisms perform the resolution, the impact on system performance is relatively small. When translating ipaddr to host name, an external mechanism such as DNS must perform the translation. This may result in significant degradation of system performance. This degradation occurs because, while seosd is waiting to receive the host name, all other processes that Privileged Access Manager has intercepted must also wait until seosd completes its processing.

- If you set the value of the under\_NIS\_server token to no, seosd allows UNIX to translate UID, GID, IP addresses, and port numbers by taking data from the following sources:

| Type of Station     | Source                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stand-alone         | seosd uses the following files for translations:<br>/etc/passwd for UID to user name<br>/etc/group for GID to group name<br>/etc/hosts for IP address to host name<br>/etc/services for service ports to service names                                                                                                                                                                                                    |
| NIS client          | The source of the information varies, depending on the operating system and its version number. The information is usually taken from /etc files and the NIS server. However, in some systems, the /etc files are not the source and the order in which translation is made is changed during system configuration. For instance, in the Solaris 2.x system the file /etc/nsswitch.conf determines the translation order. |
| DNS client          | Translation for users, groups, and services is performed using /etc files. Host names are translated by calls to the DNS server and, on some systems, the /etc/hosts file is also read.                                                                                                                                                                                                                                   |
| NIS and DNS clients | The ipaddr to host name translation is performed by DNS. For user, group, and service translations, the translations are performed in the same way as NIS client translations.                                                                                                                                                                                                                                            |

- If you set the value of the under\_NIS\_server token to yes, seosd performs its own translations. If seosd caches data for its translations, the sources of its data are as follows:

| Type of Station | Source                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NIS server      | The server machine usually behaves as both server and client, and consults the NIS server daemon for any type of translation. The files which contain the sources of the NIS resolution maps are usually located in /var/yp, but the location may vary, depending on the site configuration, and the type and version of the operating system.                                                              |
| DNS server      | The source of the information used for translation depends on the configuration of the site. DNS does not have an option to scan its resolution database; therefore, Privileged Access Manager cannot use caching, and must use a look-aside database. You must configure the look-aside database so that the utility sebuildla uses a host list file. For more information, see sebuildla in this chapter. |

|            |                     |
|------------|---------------------|
| all others | Same as DNS server. |
|------------|---------------------|

In versions 2 and higher of Privileged Access Manager, `seosd` can also use the tokens `GroupidResolution`, `HostResolution`, `ServiceResolution`, `UseridResolution`, and `resolve_timeout` to control the translation process. For more information about these tokens, see the *Reference Guide*.

## UNIX Exits

A UNIX exit is a specified program—a shell script or an executable—that runs automatically as a result of another defined Privileged Access Manager activity taking place. Privileged Access Manager supports UNIX exits when loading or unloading the Privileged Access Manager kernel module, or when issuing specific `selang` commands. For example, you can run an initialization process for each new user that you add.

A UNIX exit can run on one or more of the following occasions:

- As a pre-update exit, *before* each `selang` command that updates a *user* or *group* record
- As a post-update exit, *after* each `selang` command that updates a *user* or *group* record
- As a pre-load exit, *before* `SEOS_load` loads the kernel
- As a post-load exit, *after* `SEOS_load` loads the kernel
- As a pre-unload exit, *before* `SEOS_load -u` unloads the kernel
- As a post-unload exit, *after* `SEOS_load -u` unloads the kernel

## User or Group Record Update Exits

UNIX exits are called whenever a `selang` command that updates user or group records is executed in the UNIX environment, regardless of whether the tool is a command-line interface (`selang`) or a GUI (such as Privileged Access Manager Endpoint Management).

The term *update* refers to creating, modifying, or deleting a user or group record. Querying a user or a group does not cause any UNIX exit to run. These are the commands that can cause a UNIX exit to run:

- `newusr`
- `newgrp`
- `chusr`
- `chgrp`
- `editusr`
- `editgrp`
- `rmusr`
- `rmgrp`

From the UNIX point of view, each exit processes runs as a root process, but from the Privileged Access Manager point of view, it runs under the agent identity `_seagent`.

## How the `selang` Exit Script Works

Privileged Access Manager provides a script that you can use as a master script to call other programs according to the nature and status of the current `selang` command. The exit script that is supplied as part of Privileged Access Manager is

*ACInstallDir/exits/lang\_exit.sh* (where *ACInstallDir* is the Privileged Access Manager installation directory.) Here is how it works:

1. Privileged Access Manager automatically gives values to three parameters of the script.

| Parameter | Possible Values          |
|-----------|--------------------------|
| CLASS     | USER   GROUP             |
| ACTION    | CREATE   MODIFY   DELETE |
| STAGE     | PRE   POST               |

The parameters indicate whether Privileged Access Manager is dealing with a user or a group; whether the user or group is being created, deleted, or modified; and whether the *lang* command is about to be executed (PRE) or has just been executed (POST).

The script can pass the parameter values to programs that it calls.

| Parameter | Possible Values                                                                                                                                                                                                                                                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXEC_RV   | <p>Receives the return value of a UNIX command that you use to determine whether the exit command succeeded or failed. For PRE commands, the value is always zero. For POST commands, you can use the value to decide whether to run or skip an exit.</p> <p>For an example of how to use this parameter, locate <i>ACInstallDir/samples/exits_src</i></p> |

1. Using the CLASS and STAGE parameters, Privileged Access Manager looks for programs in the appropriate directory:

```
ACInstallDir/exits/USER_PRE/
ACInstallDir/exits/USER_POST/
ACInstallDir/exits/GROUP_PRE/
ACInstallDir/exits/GROUP_POST/
```

2. In the appropriate directory, Privileged Access Manager selects all the programs that have file names that begin with a capital S, refer to the appropriate action, and have the following format:

```
Snnaction_string
```

Where *nn* is a two-digit decimal number defining the order of the program in the execution sequence, *action* is one of CREATE, MODIFY, or DELETE, and *string* is a descriptive string.

3. Privileged Access Manager runs all the appropriate programs according to the numerical order of the second and third characters of their names.

### Example: UNIX Exit Script

You are going to delete a user, and the directory *ACInstallDir/exits/USER\_PRE/* includes the following files:

- S10CREATE\_precustom.sh
- S10DELETE\_precustom.sh
- S99DELETE\_permusrdir.sh

When you issue the command to delete the user, the first program is not run because you are deleting and not creating a user. The second and then the third programs are run in that order based on the two digits after the initial S.

## Arguments You Can Pass to `selang` Exits

When writing exits you can take advantage of the three parameters mentioned previously (CLASS, ACTION, and STAGE), and all the standard Privileged Access Manager data such as names and permissions. You can also designate extra user or group data, especially for use by the exit scripts. To store such additional data for a user or group, define it within single quotes as the value of the user's or group's UNIX APPL property in a `newusr`, `chusr`, `newgrp`, or `chgrp` command. For example:

```
chusr JONESY unix APPL('HIRED=MAY93,CLEARANCE=2')
```

Your exit program must be able to handle whatever is between the single quotes.

## Specify `selang` Exit Programs to Run

To tell Privileged Access Manager which exit programs to run, modify the [lang] section of the `seos.ini` file. Privileged Access Manager provides the `lang_exit.sh` script for pre-user, post-user, pre-group, and post-group exits. You can also specify no exit or create your own exit.

To specify your own `selang` exits, set any or all of the settings in the [lang] section of `seos.ini` as required.

### NOTE

An exit is called only if its full pathname appears as the value of an exit token.

## Example: Specify `selang` Exits

In the following example, the `seos.ini` file tokens are set so that the program `groupcheck` runs before group operations, the program `flag_exceptions` runs after group operations, the program `lang_exit.sh` runs after user operations, and no exit program runs before user operations. The `seos.ini` file tokens are set as follows:

```
[lang]

pre_group_exit = /opt/CA/PAMSC/exits/groupcheck

post_group_exit = /opt/CA/PAMSC/exits/flag_exceptions

post_user_exit = /opt/CA/PAMSC/exits/lang_exit.sh
```

## Time Out and Other Failures

Exit execution times out after 15 seconds, unless the `exit_timeout` variable in the `seos.ini` file specifies otherwise. A nonzero return value indicates failure.

- If a *pre*-update exit times out or returns a return code of greater than or equal to 16, then Privileged Access Manager kills the exit process, displays an error message, and aborts execution of the Privileged Access Manager update command. Any other positive return code does not abort the execution of the command.
- If a *post*-update exit times out or returns a nonzero value, then Privileged Access Manager kills the exit process and displays an error message. Having already been executed, the Privileged Access Manager update command remains in force.

## `selang` Exit Samples

By examining the scripts in the following directories, you can familiarize yourself with recommended scriptwriting techniques.

```
ACInstallDir/samples/exits-src
```

ACInstallDir/samples/sample\_exits

## Kernel Loader Exits

UNIX exits are called whenever the Privileged Access Manager kernel is being loaded or unloaded (SEOS\_load). This lets you define how you want to handle operating system and third-party programs when loading or unloading the Privileged Access Manager kernel. For example, you can use kernel-unloading UNIX exits to stop automatically, and later restart, processes that prevent Privileged Access Manager from unloading when running *SEOS\_load -u*.

For some operating systems, Privileged Access Manager comes with some kernel load exits, kernel unload exits, or both out of the box.

**Note:** For more information about identifying processes that prevent Privileged Access Manager kernel from unloading, see the *secons* utility in the *Reference Guide*.

## How the Kernel Loading Exits Work

To let you control operating system and third-party processes, Privileged Access Manager lets you make calls to UNIX exits automatically when loading the kernel extension.

When you run **SEOS\_load**, Privileged Access Manager does the following:

1. Looks for programs in the following directory:

```
ACInstallDir/exits/LOAD
```

2. Selects all the programs that have file names of the following format:

```
SEOS_load_string.always
```

Where *string* can be any descriptive strings.

3. Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_load_string.always -pre
```

Each file is executed with the *-pre* parameter so that you can write your exits to detect the parameter and perform the actions required before the kernel is loaded.

**Note:** If the exit returns a nonzero value, Privileged Access Manager kills the exit process, displays an error message, and aborts the kernel loading.

4. Loads the kernel (SEOS\_syscall).
5. Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_load_string.always -post
```

Each file is executed with the *-post* parameter so that you can write your exits to detect the parameter and perform the actions required after the kernel is loaded.

**Note:** If the exit returns a nonzero value, the product kills the exit process and displays an error message. Having already been loaded, the kernel remains loaded.

## How the Kernel Unloading Exits Work

To let you control operating system and third-party processes, Privileged Access Manager lets you make calls to UNIX exits automatically when unloading the kernel extension.

When you run **SEOS\_load -u**, Privileged Access Manager performs the following actions:

1. Looks for programs in the following directory:

ACInstallDir/exits/LOAD

2. Selects all the programs that have file names of the following format:

```
SEOS_unload_string.always
```

where *string* can be any descriptive strings.

3. Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_load_string.always -pre
```

Each file is executed with the *-pre* parameter so that you can write your exits to detect the parameter and perform the actions required before the kernel is unloaded.

**Note:** If the exit returns a nonzero value, Privileged Access Manager kills the exit process, displays an error message, and aborts the kernel unloading.

4. Tries to unload the kernel, if the kernel *does not* unload: Selects all the programs that have file names of the following format:

```
SEOS_unload_string.opt
```

Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_unload_string.opt -pre
```

Each file is executed with the *-pre* parameter so that you can write your conditional exits to detect the parameter and perform the additional optional actions required before the kernel is unloaded.

**Note:** If the exit returns a nonzero value, then the product kills the exit process, displays an error message, and aborts the kernel unloading, unloads the kernel. Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_unload_string.opt -post
```

Each file is executed with the *-post* parameter so that you can write your conditional exits to detect the parameter and perform the additional optional actions required before the kernel is unloaded.

**Note:** If the exit returns a nonzero value, then the product kills the exit process and displays an error message. Having already been unloaded, the product kernel remains unloaded.

```
SEOS_unload_string.opt
```

Executes, in lexicographical order, each file it found in the directory *ACInstallDir/exits/LOAD*:

```
SEOS_unload_string.always -post
```

Each file is executed with the *-post* parameter so that you can write your exits to detect the parameter and perform the actions required after the kernel is loaded.

**Note:** If the exit returns a nonzero value, the product kills the exit process and displays an error message. Having already been unloaded, the product kernel remains not loaded.

## Interact with LDAP

This topic describes ways that Privileged Access Manager interacts with LDAP.

### Transfer User Names

If you are using both Privileged Access Manager and LDAP, you can transfer user names between them using scripts of your own design. Three sample scripts are provided.

## WARNING

**Warning:** To set up sebuildla and the required LDAP configuration settings, execute the ldapsearch command. We recommend that you read the man pages for ldap(1), ldapsearch(1), and the information about setting up in the documentation for your LDAP client.

Two of the provided scripts--ldap2seos and seos2ldap--export whole sets of users from Privileged Access Manager to an LDAP server and imports them from an LDAP server to Privileged Access Manager.

A third sample script, S50CREATE\_Ldap\_u.sh, automatically transfers new UNIX user names from Privileged Access Manager to LDAP as they are created.

The sample scripts require access to a TCL shell environment; they use the Language Client API (LCA) library extension, [tcllca.so](#).

**Note:** For more information about LCA and the TCL extension, see the Language Client API and the appendix the LCA Extension respectively in the *SDK Guide*.

If you do not have TCL, consult the FAQ posted monthly to comp.lang.t\_c\_l by Larry Virden. The FAQ is available on the MIT website and the Terafirm website.

You can also refer to the Sun website for TCL news, documentation, and resources.

### **S50CREATE\_Ldap\_u.sh**

S50CREATE\_Ldap\_u.sh uploads new UNIX users to LDAP as they are created.

Privileged Access Manager supplies a sample shell script to import new UNIX users automatically to an LDAP server. The script that you need can vary from the sample.

To employ the sample shell script, assuming that you are already using the provided exit script, follow these steps:

1. Copy the S50CREATE\_Ldap\_u.sh file to the directory *ACInstallDir/exits/USER\_POST*. In this directory, the script becomes a post-user exit.
2. In the seos.ini file in the [ldap], set the base\_entry token to the LDAP base entry.  
For example, for an organization that is named ServerWorld, located in Canada, the base entry might be:  
o=ServerWorld, c=CA.
3. In the same section, set the host name to the host name of the LDAP server. Set the path to the LDAP base directory.  
(The sample script looks for the line command utilities in the bin directory under that directory.)

Common Names (cn) are derived from the full name of the user. If the Privileged Access Manager database contains only the user name and surname, for example, these names comprise the Common Name. You are locked into the Common Name, so we recommend that you do not base it on a user name.

Each user then added to UNIX with selang is automatically uploaded to the LDAP server. If the user already exists in LDAP, an error message results.

When you add users with this script, the relevant LDAP replies and any warnings are collected in the /tmp/add\_User2Ldap.tcl.log file. You can examine this file, using vi or any other standard UNIX editor, to check for errors. The file is overwritten with the new set of replies and warnings each time you add new users.

## NIS Configuration

Privileged Access Manager intercepts requests to access system resources and decides whether to permit or deny these requests. The decision is based on access rules and policies that are defined in the database. The interception of requests to access system resources takes place at the kernel level.

To control hosts, groups, users, and services, the kernel and the relevant system calls use codes or numbers instead of names. Examples: IP addresses, group IDs, service numbers. Privileged Access Manager defines access rules based on



names. Privileged Access Manager translates names into codes recognizable by the kernel. This process is called name resolution.

On stand-alone stations, except for stations running Sun Solaris 2.5 or higher, name resolution is completed directly through the local user, group, and host files (`/etc/passwd`, `/etc/group`, and `/etc/hosts`). When Privileged Access Manager resolves a name, it simply calls a system function that in turn reads the relevant file.

On larger networks, however, this information is seldom stored locally. When you use NIS, DNS, or both, there are no local files that you can consult during name resolution. The information is requested and received from a server over the network.

## Avoid Deadlocks with the Lookaside Database

The setting of the `under_NIS_server` token in the `seos.ini` configuration file has a default setting of yes to avoid deadlocks. The token tells Privileged Access Manager to use its own internal name resolution tables instead of NIS, DNS, or the `nsdc` cache. Unless otherwise specified, these tables reside in memory.

Privileged Access Manager internal name resolution is much faster than NIS name resolution and even faster than using files. Using Privileged Access Manager internal name resolution improves performance even in an environment where there is no danger of deadlocks.

### NOTE

No cache exists for the internal name resolution tables in the lookaside database. Privileged Access Manager uses an open file handle to read data from the tables.

## Store Resolution Tables on Disk

Privileged Access Manager name resolution tables are generated while it is starting up. Maintain the tables on disk, not in memory, because storage in memory can lead to memory overload. Also, when the information is read into memory, it is static. Because it is static, Privileged Access Manager would not know of any changes made to user, group, or host information. The only way to update the tables in memory is to restart Privileged Access Manager.

To keep data current, Privileged Access Manager provides a lookaside database that ensures internal name resolution tables are stored on disk.

### NOTE

To implement the lookaside database, use `seos.ini` configuration settings. For more information about `seos.ini` configuration settings, see the *Reference Guide*.

## Set Up the Lookaside Database

The four tables in the lookaside database are `userdb.la`, `groupdb.la`, `hostdb.la`, and `servdb.la`. These four tables handle user, group, host, and service name resolution requests. The tables are located in the directory specified by the `lookaside_path` token in the `seos.ini` file, which by default is `/opt/CA/PAMSC/ladb`.

### Lookaside Database with Four Tables

To set up the lookaside database with four tables, do one of the following:

- If you are installing Privileged Access Manager, answer yes when asked if you want to create the lookaside database.
- If you already installed Privileged Access Manager:
  - a. In the `[seosd]` section of `seos.ini` change the following tokens to **yes**:
    - a. `under_NIS_server`
    - b. `use_lookaside`
  - b. Run `sebuildla -a` to create all four tables.

## Lookaside Database with Less Than Four Tables

You can also create one, two, or three tables. For example, if you want to use the lookaside database to resolve hosts only, complete the following steps:

1. After you install Privileged Access Manager, change the following tokens in the [seosd] section of the seos.ini file:
  - Set under\_NIS\_server to blank.
  - Set HostResolution to ladb.
2. Run sebuildla -h to create a table of all hosts, including local and DNS hosts.  
or  
Run sebuildla -e to create a table of local hosts only (defined in /etc/hosts).

To create a lookaside database with other tables, use the appropriate tokens in the seos.ini file and then run the appropriate option with sebuildla.

### NOTE

For descriptions of these tokens, see the seos.ini initialization file in the *Reference Guide*. For more information about sebuildla, see the *Utilities Guide*.

### WARNING

Run sebuildla whenever you add a host.

## How the Lookaside Database Works

The four tables in the lookaside database (groupdb.la, hostdb.la, servdb.la, and userdb.la) contain resolution information for groups, hosts, services, and host names. The tables are located in the directory specified by the lookaside\_path token in the seos.ini file, which by default is /opt/CA/PAMSC/ ladb.

Privileged Access Manager internal name resolution is much faster than NIS name resolution and even faster than looking up the files.

## Implement the Lookaside Database

### NOTE

The problems and solutions outlined here are for informational purposes only. Actual settings are correct upon installation and most users need not take any action.

Here is a broad overview of how Privileged Access Manager implements the lookaside database:

- The relevant tokens in the seos.ini file are set.
- The relevant symbolic links in the /opt/CA/PAMSC/exits directory are defined.
- The command /opt/CA/PAMSC/bin/sebuildla -a was issued to build the lookaside database.

The sebuildla utility taps into the native resolution mechanisms such as the files and NIS to build the lookaside database.

No security-sensitive information (such as password, location of the home directory, or gecost) is kept in the lookaside tables. The lookaside database tables contain only a numeric ID number and a name.

Once the lookaside database is created, update it using the sebuildla utility. You do *not* need to restart Privileged Access Manager.

## Update the Hosts Lookaside Table

You must update the hosts' lookaside table. To do so, execute sebuildla -h at regular intervals (site-specific). Use cron jobs to do this.

Every time you change the UNIX user or group databases utilizing selang, you must run the sebuildla utility. Privileged Access Manager provides exit scripts for this purpose, which runs sebuildla with the appropriate parameters.

## Name Resolution on an NIS DNS Client

Privileged Access Manager performs name resolution on a client-only NIS or DNS station (which is not its own server) as follows:

1. Privileged Access Manager generates a network request to connect to the relevant server.
2. The Privileged Access Manager kernel extension intercepts the request.
3. The Privileged Access Manager kernel extension permits the request because it knows that the request was made internally.
4. A connection to the NIS or the DNS server is established and the information necessary for name resolution is retrieved.
5. Once the name is resolved, Privileged Access Manager continues the process of deciding whether to permit or deny the original access request.

A standard Privileged Access Manager configuration is sufficient to handle name resolution on a client server.

## Name Resolution on a Server Deadlock

Privileged Access Manager performs name resolution on a server that includes itself as a client as follows:

1. Privileged Access Manager generates a network request to connect to the relevant server.
2. The kernel extension intercepts this request.
3. The kernel extension permits the request because it knows that the request was made internally by the Privileged Access Manager process.
4. The NIS or DNS server (which is located on the same station) generates a request to accept the network connection.
5. The kernel extension intercepts this request.
6. The kernel extension knows that a Privileged Access Manager process did not make this request. It places this request on the queue of requests awaiting seosd decision.
7. The seosd daemon is now caught in a deadlock. It is waiting for the reply necessary to complete name resolution, but the process that should provide this reply cannot proceed until seosd gives it permission to accept the network connection. The first request generates the second, and creates a deadlock.

## Name Resolution on Sun Solaris Deadlock

Name resolution on Sun Solaris entails accessing the *nscd* cache. The *nscd* is a process that provides a cache for the most common name service requests. The *nscd* furnishes caching for the *passwd*, *group*, and *hosts* databases.

The cache is not permanent. It becomes invalid as changes are made to the *passwd*, *group*, and *hosts* databases, or as the time-to-live stamp expires.

The Sun Solaris setup can create a deadlock like the one described in the previous section. Here, the interaction between Privileged Access Manager and the *nscd* process causes the deadlock.

1. During name resolution, Privileged Access Manager accesses the *nscd* cache.
2. The *nscd* process can decide that the cache is too old. In this case, it attempts to refresh the information by accessing the *passwd*, *group*, and *hosts* databases (locally or on a server).
3. The request to access these databases is intercepted by the kernel extension. Since a Privileged Access Manager process is not making the request, it is placed on a queue awaiting seosd decision. But no such decision is possible because seosd is still engaged in the previous request. The first request generates the second, and creates a deadlock.

## Restricting Local Interprocess Communication over UNIX (LOCAL) Named Domain Sockets

**Note:** This functionality is not supported in the Endpoint-Management UI.

In addition to controlling interprocess communication (IPC) over TCP, Privileged Access Manager can also restrict local IPC which uses UNIX (or LOCAL) named domain sockets. Privileged Access Manager intercepts processes that attempt to connect to a socket using the named socket path. You can write Privileged Access Manager rules to authorize connections to the socket using the UNIX\_SOCKET class and connect (c) access.

### Example

This example enables the user root full access and enables the user John to run docker commands. Docker commands communicate with the docker daemon using UNIX domain sockets as the default communication through socket path /run/docker.sock

```
so class+(UNIX_SOCKET)

nr UNIX_SOCKET /run/docker.sock owner(nobody) defaccess(none) audit(all)

auth UNIX_SOCKET /run/docker.sock uid(root) access(all)

auth UNIX_SOCKET /run/docker.sock uid(john) access(c)
```

The user John can now run docker commands using docker default local communication. Example: `sudo docker run hello-world`. Another user, Chris, cannot run such docker commands, and root maintains full capabilities.

## Protect Process being Attached by Other Processes

**Note:** In this release, this functionality is not supported in the Endpoint-Management UI.

System-related processes can be tampered with without the knowledge of the administrator using malicious code. To overcome this issue, this release of the product has enhanced the PROCESS class with an attribute called ATTACH.

The ATTACH attribute of the PROCESS class protects the process from being attached by other processes through the ptrace system calls. With this attribute, you can authorize which process should access a specific process.

The following example describes the use of the ATTACH attribute:

### Follow these steps:

1. Consider top as an example process with the following executable path:

```
/usr/bin/top
```

2. Create a record for the process top using the following code:

```
PAMSC> nr process /usr/bin/top owner(nobody) defacc(n)
```

A record is created for the process /usr/bin/top using the PROCESS class with owner as nobody and default access as none. At this time, the process top /usr/bin/top cannot be attached by any other process.

3. You can authorize the process /usr/bin/top to be attached to any other process running under root using the following Selang rule:

```
PAMSC>auth process /usr/bin/top uid(root) access(attach)
```

## Endpoint Administration for Windows

This guide describes the concepts used by Privileged Access Manager for Windows--a product that provides a total security solution for open systems. The guide describes Windows endpoint management tasks and concepts.

- [Manage Endpoints \(Windows\)](#)
- [Expand Native Security](#)
- [Components](#)
- [Users and Groups](#)
- [Where Information about Accessors Is Stored](#)
- [Guidelines for Managing Accessors in Enterprise Stores](#)
- [Database Accessors](#)
- [Classes](#)
- [Windows Services Protection](#)
- [Windows Registry Protection](#)
- [Protect File Streams](#)
- [Internal File Protection \(Windows\)](#)
- [Manage Authorization](#)
- [User Impersonation Protection](#)
- [Set Up the Surrogate DO Facility](#)
- [Define SUDO Records \(Task Delegation\)](#)
- [Check User Inactivity](#)
- [Security Auditors](#)
- [Events Interception](#)
- [Types of Intercepted Events](#)
- [Warning Mode](#)
- [Monitor Access Control Activity](#)
- [What CA Privileged Access Manager Server Control Audits](#)
- [The Auditing Process](#)
- [How Auditing Works for Interception Events](#)
- [View Audit Event Logs](#)
- [The Audit Log \(Windows\)](#)
- [Group Authorization](#)
- [Ownership](#)
- [Authorization Examples](#)
- [Sub Administration](#)
- [Environmental Considerations](#)
- [Default Permissions to Access the Database](#)
- [Native Permissions to Access the Database](#)
- [Policy Model Database \(Windows\)](#)
- [Automatic Rule-based Policy Updates](#)
- [Update Subscribers](#)
- [Mainframe Password Synchronization](#)
- [Toggle Driver Interception](#)
- [Disable CA Privileged Access Manager Server Control Kernel Interceptions](#)
- [Stack Overflow Protection](#)
- [Configure Settings](#)

## **Manage Endpoints (Windows)**

Privileged Access Manager is a software product that is an active, comprehensive security software solution for Open Systems, tied dynamically to the operating system. Each time a user requests a security-sensitive operation, such as

opening a file, substituting a user ID, or obtaining a network service, Privileged Access Manager can intercept the event in real time. The product evaluates its validity before passing control to the standard operating system (OS) functions.

### **What Is Privileged Access Manager? (Windows)**

Privileged Access Manager provides you with a powerful tool for managing security for your native platforms, making it possible to implement a security policy that can be customized entirely to the security requirements of the enterprise. Privileged Access Manager lets you provide security for users, groups, and resources beyond what is available in native operating systems. The product lets you centrally manage security across the organization and integrate your Windows and UNIX security policies in a heterogeneous environment.

### **What Is Protected? (Windows)**

Privileged Access Manager protects the following entities:

- **Files**

Is a user authorized to access a particular file?

Privileged Access Manager restricts the ability of a user to access a file. You can give a user one or more types of access, such as READ, WRITE, EXECUTE, DELETE, and RENAME. The access can be specified regarding an individual file or to a set of similarly named files.

- **Terminals**

Is a user authorized to use a particular terminal?

This check is done during the login process. Individual terminals and groups of terminals can be defined in the Privileged Access Manager database, with access rules that state which users, or groups of users, are allowed to use the terminal or terminal group. Terminal protection ensures that no unauthorized terminal or station can be used to log in to the accounts of powerfully authorized users.

- **Sign-on time**

Is a user authorized to log on at a particular time on a particular day?

Most users use their stations only on weekdays and only during work hours; the time-of-day and day-of-week login restrictions, as well as holiday restrictions, provide protection from hackers and from other unauthorized accessors.

- **TCP/IP**

Is another station authorized to receive TCP/IP services from the local computer? Is another station authorized to supply TCP/IP services to the local computer? Is another station permitted to receive services from every user of the local station?

An open system is a system in which both the computers and the networks are open. The advantage of an open system is also a disadvantage. Once a computer is connected to the outside world, you can never be sure who enters the system and what damage an alien user can do, intentionally or by mistake. Privileged Access Manager includes firewalls that prevent local stations and servers from providing services to unknown stations.

- **Multiple login privileges**

Is the user permitted to log in from a second terminal?

The term *concurrent logins* refers to a user's ability to be logged onto the system from more than one terminal.

Privileged Access Manager can prevent a user from logging in more than once. This prevents intruders from logging into the accounts of users who are already logged in.

- **User-defined entities**

You can define and protect both regular entities (such as TCP/IP services and terminals) and functional entities (known as *abstract* objects; such as performing a transaction and accessing a record in a database).

- **Aspects of administrator authority**

Privileged Access Manager provides the means to both delegate superuser authorities to operators and restrict the privilege of the superuser account.

- **Registry keys**

Is a user authorized to access a particular registry key?

Privileged Access Manager restricts the ability of a user to access registry keys. You can give a user one or more types of access, such as READ, WRITE, and DELETE. The access can be specified with regard to an individual registry key or to a set of similarly named registry keys.

- **Programs**

Can a particular program be trusted? Is the user authorized to invoke it? Can the user access a specific resource using a program?

The security administrator can test programs to ensure that they do not contain any security loopholes that can be used to gain unauthorized access. Programs that pass the test and are considered safe are defined as trusted programs. The Privileged Access Manager self-protection module (also referred to as the **watchdog**) knows which program is in control at a particular time and checks whether the program has been modified or moved since it was classified as trusted. If a trusted program is modified or moved, the program is no longer considered trusted and Privileged Access Manager does not allow it to run.

In addition, Privileged Access Manager protects against various deliberate and accidental threats, including:

- **Kill attempts**

Privileged Access Manager can be used to protect critical servers and services or daemons against kill attempts.

- **Password Attack**

Privileged Access Manager protects against various types of password attacks, enforces the password-definition policies of your site, and detects break-in attempts.

- **Password Delinquency**

Privileged Access Manager policies delineate rules that force users to create and use passwords of sufficient quality. To ensure that users create and use acceptable passwords, Privileged Access Manager can set maximum and minimum lifetimes for passwords, restrict certain words, prohibit repetitive characters, and enforce other restrictions. Passwords are not permitted to last too long.

- **Account Management**

Privileged Access Manager policies ensure that dormant accounts are dealt with appropriately.

### ***How Is It Protected? (Windows)***

Privileged Access Manager starts immediately after the operating system finishes its initialization. The product places hooks in system services that must be protected. In this way, control is passed to Privileged Access Manager before the service is performed. Privileged Access Manager decides whether the service can be granted to the user.

For example, a user may attempt to access a resource protected by Privileged Access Manager. This access request generates a system call to the kernel to open the resource. Privileged Access Manager intercepts that system call and decides whether to grant access. If permission is granted, Privileged Access Manager passes control to the regular system service. If Privileged Access Manager denies permission, it returns the standard permission-denied error code to the program that activated the system call, and the system call ends.

The decision is based on access rules and policies that are defined in the database. The database describes two types of objects: accessors and resources. *Accessors* are users and groups. *Resources* are objects to be protected, such as files and services. Each record in the database describes an accessor or a resource.

Each object belongs to a class—a collection of objects of the same type. For example, **TERMINAL** is a class containing objects that are terminals (workstations) protected by Privileged Access Manager.

### ***Class Activation (Windows)***

The information about class status (that is, whether the class was active or inactive) is held in the database. Every attempt to access a resource is intercepted by Privileged Access Manager, which checks the status in the database. If the class is inactive, access is allowed without further checking for authorization.

Privileged Access Manager issues a list of active classes when the engine starts and when a user changes the class activity status. If a class is inactive, access to the resource is not intercepted, which reduces overhead.

### ***Accessor Elements (Windows)***

Each user is represented by an *accessor element* (ACEE)—an in-memory reflection of the record for the user in the database. Privileged Access Manager builds the accessor element during the login process. The accessor element is associated with the process of the user. Whenever the process requests a system service that is protected by Privileged Access Manager, or issues an implicit request to access a resource, the product accesses the record of the resource. It then determines whether the information in the previously created accessor element—such as the user's security level, mode, and group—lets the user access the resource.

### How Instrumentation Works

*Instrumentation* is a method that enables Privileged Access Manager to monitor, track, and change the execution flow of applications. Instrumentation enables Privileged Access Manager to monitor system processes, intercept, and implement a proprietary module in the application address space.

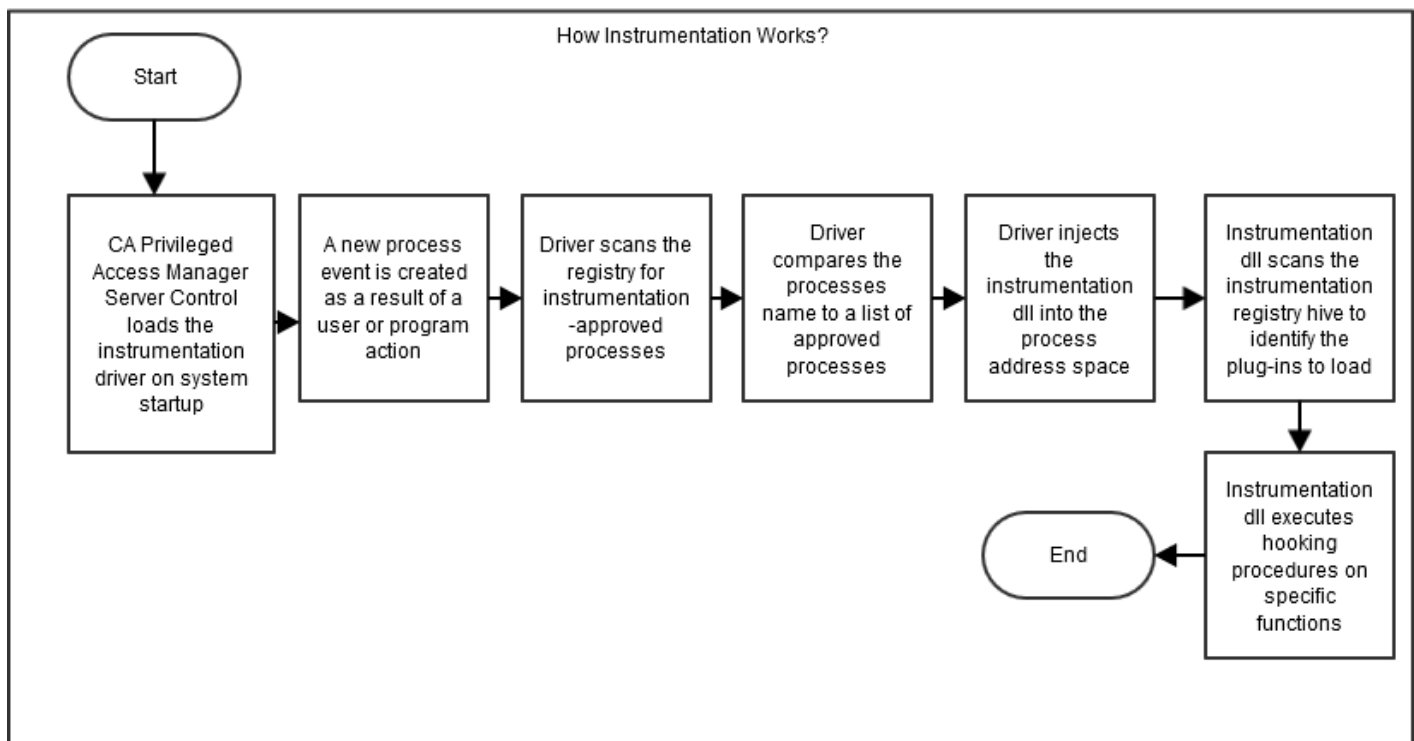
The instrumentation process consists of two phases: the *kernel instrumentation* phase and the *user-mode instrumentation* phase.

#### NOTE

For more information about kernel and user-mode interceptions, refer to the [User Impersonation Protection](#) chapter.

The following diagram illustrates the instrumentation process:

**Figure 44: Instrumentation\_Process**



In the kernel instrumentation phase, Privileged Access Manager performs the following actions:

1. Privileged Access Manager loads the instrumentation driver (cainstrm.sys) on system startup.
2. A new process event is created as a result of a user or program action.
3. In fixed intervals the instrumentation driver scans the registry hive for instrumentation-approved processes.  
You specify the list of instrumentation-approved processes using the instrumentation ApplyonProcesses [registry key](#).



4. When Privileged Access Manager identifies a new process event, it searches for the processes name in the list of approved processes. If found, the driver injects the instrumentation dll into the process address space.

In the user-mode instrumentation phase, Privileged Access Manager performs the following:

1. The instrumentation dll scans the instrumentation registry hive to identify the plug-ins to load into the process address space and does one of the following steps:
  - Loads all listed plug-ins in to the processes memory address. Continues to step 2.
  - Unloads itself if no plug-ins are listed.
2. Privileged Access Manager executes hooking procedures based on the specific functions that each plug-in contains using the Microsoft Detours library.  
Microsoft Detours is a library for instrumenting Win32 functions. For more information about Microsoft Detours, see the [Microsoft Detours web site](#).

### **WARNING**

If instrumentation is disabled, the following features or applications do not work:

- [STOP](#)
- WinService
- Configuration of Windows batch files as a PROGRAM object
- Database/IIS integration with SAM
- [RunAs](#)

## **Expand Native Security**

The following Privileged Access Manager features expand native security.

### **Superuser Account Limitations**

Users who administer and manage operating systems are typically members of predefined accounts. These accounts are automatically created during the system setup. Examples of these accounts are the root account on UNIX systems and the Administrator account on Windows systems. Each of the predefined accounts exists to perform a certain set of system functions.

For example, users acting as root or Administrator can create, delete, and modify users and lock, reconfigure, and shut down servers.

One of the major security risks is that an unauthorized user gains control of these accounts. If this happens, the user can seriously damage the system.

Privileged Access Manager lets you limit the rights that are granted to these accounts and limit the rights of members of user groups that have these accounts as members. These limits reduce the vulnerability of your operating system.

### **Privileged Access Manager Administrators**

When you install Privileged Access Manager, you are asked to name one or more product administrators. Administrators have the authority to modify all or part of the rules database. You need at least one full-authority administrator. This administrator can modify or create access rules freely and can designate other levels of administrators.

Once you have defined users for your system, assign administrative authority to other users by assigning the ADMIN attribute to them.

### **NOTE**

A user with the ADMIN attribute possesses powerful authority. Therefore, limit the number of ADMIN users. A good policy is to separate the roles of the native superuser and ADMIN. Remove the ADMIN attribute from the superuser after you have set up one or more Privileged Access Manager security administrators.

Because you need at least one user with authority to manage the database, Privileged Access Manager does not let you delete the last user that has the ADMIN attribute.

If you expect any of the product administrators to administer other hosts from this workstation, ensure that a rule in the database on that host gives them READ and WRITE access from this workstation.

### **Sub Administration**

Privileged Access Manager contains a *sub administration* feature. This feature lets administrators grant specific privileges that enable regular users to manage specific classes. These users are then named sub administrators.

For example, you can allow a specific user to manage users and groups only.

You can also specify a higher level of sub administration. To specify this level, grant access not only for specific classes, but for specified records in these classes.

### **Administration Rights for Regular Users**

Privileged Access Manager lets you grant ordinary users (non-administrators) the necessary rights and privileges to perform administrative tasks without being members of the Administrators group. The ability to delegate tasks by granting administrative privileges in this granular way is a significant advantage of Privileged Access Manager.

- A record in the SUDO class stores a command script to allow users to run the script with borrowed permissions.
- The data property value is the command script. This value can be modified by adding to it optional script parameter values.
- Each record in the SUDO class identifies a command for which a user can borrow permissions from another user.
- The key of the SUDO class record is the name of the SUDO record. This name is used instead of the command name when a user executes the commands in the SUDO record.

### **Enhanced File Protection**

Privileged Access Manager supports both logical and absolute file name formats. For example, if the file foo.txt is located under the directory \tmp on the logical drive D and the logical name D: is assigned to physical disk 1, partition 0, you can use either the logical or absolute file name to define a file to the product database:

```
nr file D:\tmp\foo.txt
```

or

```
nr file \Device\HardDisk1\Partition1\tmp\foo.txt
```

#### **NOTE**

If the second format is used, the file remains protected even if the logical name of the disk is changed. The absolute file name format is also supported for Privileged Access Manager generic file protection.

The product protects all file systems that are currently used in supported Windows operating systems. The two most commonly used are the Windows file system (NTFS) and the file allocation table (FAT).

The product also supports CDFS (a file system especially for CDs).

The product supplies a total security solution to the file allocation table (FAT) and an extra layer of security to other file systems including NTFS and CDFS.

### **Generic File Protection**

Privileged Access Manager supports both logical and absolute file names. The absolute file name format is also supported for Privileged Access Manager generic file protection.

Generic file protection lets you protect all the files that fit a specified wildcard pattern (regular expression). Any resource with a name matching the specified wildcard pattern is protected by the specified generic access rule. The product lets you protect files generically.

If a resource matches more than one generic access rule, Privileged Access Manager chooses the rule that most closely matches the file.

With generic file protection, no more than a handful of security rules must be defined to protect many of the files requiring protection.

## **Password Protection**

Native Windows security can protect passwords and can enforce password quality in a number of ways. Windows offers the ability to:

- Enforce a maximum password age
- Enforce a minimum password length
- Save up to 24 generations of the passwords of a user
- Lock out accounts after repeated login failures
- Force users to log in to Windows before changing their passwords

Privileged Access Manager also enforces the same rules but through its own unique mechanisms. In addition, the product implements two-way password synchronization with mainframe computers.

## **Enhanced Password Protection**

Native Windows security provides a significant amount of [protection for user passwords](#). However, Privileged Access Manager significantly extends password protection so that the likelihood of a hacker succeeding in stealing a password is greatly reduced.

When using Privileged Access Manager, you can create more rules that force users to choose safer, more secure passwords. For instance, you can demand that users select a minimum number of alphabetic, numeric, special, lowercase, or uppercase characters. You can also ensure that the new password that a user selects does not contain, and is not contained by, the password being replaced.

## **Program Pathing**

*Program pathing* is an access rule that is associated with a file that requires that the file is accessed only through a specific program. Program pathing greatly increases the security of sensitive files. Privileged Access Manager lets you use program pathing to provide more protection for the files in your system.

## **B1 Security Level Certification**

Privileged Access Manager includes the following B1 Orange Book features: security levels, security categories, and security labels.

- Accessors and resources in the database can be assigned a *security level*. The security level is an integer between 1 and 255. An accessor can gain access to a resource only if the accessor has a security level equal to or greater than the security level assigned to the resource.
- Accessors and resources in the database can belong to one or more *security categories*. An accessor can access a resource only if the accessor belongs to all of the security categories assigned to the resource.
- A *security label* is a name that associates a particular security level with a set of zero or more security categories. Assigning a user to a security label gives the user both the security level and any security categories associated with the security label.

### **NOTE**

For more information about B1 Orange Book features, see the *Implementation Guide*.

## Set Up Audit Procedures

Privileged Access Manager keeps audit records for events of access denial and access grants according to the audit rules defined in the database. The decision whether to log a certain event is based on the following rules:

- Every accessor and resource has an AUDIT property that can be set to indicate whether access successes, failures, or both, are logged. In addition, the AUDIT property for accessors can indicate whether login successes, failures, or both are logged.
- If the resource or the accessor has the AUDIT(ALL) attribute, all events concerning resources that are protected by Privileged Access Manager are logged, regardless of whether access failed or succeeded.
- If the access to a resource protected by Privileged Access Manager is successful and the user or the resource has AUDIT(SUCCESS), the event is logged.
- If the access to a resource protected by Privileged Access Manager fails and the user or the resource has AUDIT(FAIL), the event is logged.

Only a system auditor, a user to whom the AUDITOR attribute is assigned, can perform auditing tasks such as changing the auditing attribute that is assigned to users and resources.

If a resource is in warning mode, any access that violates access rules for the resource results in a warning mode audit record, which states that Privileged Access Manager permitted access to the resource.

The audit records constitute a file that is called the *audit log* (seos.audit). The location for the audit log is specified in the registry, as is the location for the error log.

The audit log (and also the error log) is specified under the following registry key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\logmgr
```

The audit log is a binary file and cannot be edited or changed. However, you can use Privileged Access Manager Endpoint Management to view recorded events, to filter out events by time restrictions or event type, and so forth. (You can also use the seaudit utility to accomplish these same tasks.)

Consider archiving (backing up) old audit logs and error logs to let you scan the events at a later date.

## Components

Privileged Access Manager includes the following components:

- A database (seosdb)
- Two drivers (seosdrv and drveng)
- Several services, including the Watchdog, the Agent, the Engine (seosd), the Policy Model, and Task Delegation
- A graphical user interface

### Database

The database contains definitions of the following elements:

- Users and groups in your organization
- System resources that need protection
- Rules governing user and group access to system resources

### Drivers

The drivers protect all the Privileged Access Manager files and registry keys by performing the following tasks:

- Intercepting every request to open a file or registry key, terminate a process, and perform network activities.
- Passing these requests to the Privileged Access Manager Engine and receiving the decision about whether the request is granted or denied.
- Forwarding the decision to the original system call of the operating system. The operating system then continues its processing that is based on the answer it received from the drivers.

## **Services**

### ***Watchdog***

The Watchdog constantly checks that the other Privileged Access Manager services are running. On the rare occasion when the Watchdog discovers that another service has stopped, it immediately starts the service again.

### ***Agent***

The Agent is responsible for the following tasks:

- Communicating with Privileged Access Manager clients through a proprietary application protocol above TCP/IP
- Managing security for the Privileged Access Manager user

### ***Engine***

The Engine is responsible for the following tasks:

- Managing the database, including controlling all database updates
- Deciding whether to grant access requests that it receives from the Driver and the Agent
- Checking that the Watchdog service is running, and restarting the Watchdog if it discovers that the Watchdog has stopped running

The Engine handles database access requests *and* makes the access decision, creating an efficient service.

### ***Policy Model***

Managing tens or hundreds of databases individually is not practical. Therefore, Privileged Access Manager supplies the Policy Model service, a component that permits management of many computers from one computer. Using the Policy Model service is optional, but it greatly simplifies administration at large sites.

With the Policy Model service, use a Policy Model database (PMDB). Like other Privileged Access Manager databases, the PMDB contains users, groups, protected resources, and rules governing access to the resources. In addition, the PMDB contains a list of subscriber stations. A subscriber station is one linked to the PMDB so that any change to the PMDB is automatically sent to the subscriber database.

You can create a basic security policy for your organization and can implement all the necessary rules on a single database, the Policy Model database. The subscribers can include both Windows and UNIX stations, ensuring uniform rules with minimal administrative effort.

The system or security administrator updates the PMDB. The PMDB then propagates all updates from the PMDB to its subscribers in batch mode, freeing the administrator for other work.

A PMDB can have two types of subscribers: another PMDB or a local database. This PMDB also contains a list of subscribers to which it propagates database updates. This feature lets you build a hierarchy of PMDBs. The local database can be used to protect the users, groups, and resources that are defined on the station.

## **selang**

The command-line language, *selang*, performs all the functions of Privileged Access Manager. To use *selang* commands, open a Command Prompt window and start *selang*. You can also use *selang* in scripts.

For more information about *selang* and its commands, see the chapter "The *selang* Command Language" in the *Reference Guide*.

## Endpoint Management

Privileged Access Manager provides two ways to let you manage the resources in your enterprise and control who has access to them:

- **selang:** The Privileged Access Manager command language  
The selang command language lets you make definitions in the Privileged Access Manager database. The selang command language is the command definition language.

### NOTE

For more information about using selang, see the *selang Reference Guide*.

- **Privileged Access Manager Endpoint Management:** The endpoint administration interface  
The web-based interface lets you administer remote endpoints through a central administration server.

### NOTE

For more information about installing Privileged Access Manager Endpoint Management, see the *Implementation Guide*.

## Users and Groups

In Privileged Access Manager, every action and access attempt is performed on behalf of a user. The user is held responsible for submitting the request. Every process in the system is therefore associated with a certain user name. The user name identifies the user to Privileged Access Manager.

A *user* is a person who can log on, or can be the owner of a batch or daemon program. In Privileged Access Manager, a user performs every access attempt. Privileged Access Manager can use user information from the product database and from the enterprise user stores. The product stores user information in its database, in either a USER record or an XUSER record.

### NOTE

An *enterprise user store* is a store in the operating system that stores users or groups. Example: /etc/passwd and /etc/groups on UNIX systems, or Active Directory on Windows.

A *group* is a collection of users. A group defines common access rules for users in the group. Groups can be nested (belong to other groups). Privileged Access Manager can use group information from the Privileged Access Manager database and from the enterprise user stores. Typically, you create groups and assign users to them, based on a role; for example, database\_administrators.

The user records are the key accessor records. The main purpose for using groups in Privileged Access Manager is to assign access authorities to all users in group at one time. Assigning access authorities at one time is easier and less error prone than assigning them separately to each user.

## Where Information about Accessors Is Stored

The information that Privileged Access Manager uses about users and groups is stored both in the product database and in the host operating system. The host operating system information stores are called *enterprise user stores*, or just *enterprise stores*. By default, Privileged Access Manager is configured so that it does not use the enterprise stores. You can configure Privileged Access Manager so that it looks for information and uses information from the users and the group memberships defined in the enterprise store. This is useful if the product cannot find a user or group defined in its own database.

### NOTE

Privileged Access Manager uses information from the enterprise stores but only writes to them if you use selang commands in the native environment.

When checking for authorization, Privileged Access Manager always checks for accessors that are defined in its own database before it checks the enterprise store: if you have an enterprise user with the same name as a user defined in the product database, Privileged Access Manager ignores the enterprise user.

### **How Privileged Access Manager Finds a User Record**

When a user logs in, Privileged Access Manager conducts the search in the following order, until it finds a record associated with the user. Privileged Access Manager:

1. Searches for a user defined in its database.
2. Searches its cache for an enterprise user of that name. When the network is down, the operating system (OS) lets users log in using the OS cached credentials. The purpose of the Privileged Access Manager cache is to let the product use the records of enterprise users in these cases.
3. Uses the operating system to search the enterprise user stores for a user of that name.
4. If Privileged Access Manager does not find a record that is associated with the user in its database or in the enterprise stores, it assigns the user the attributes in the `_undefined USER` record.

### **Integration with the Enterprise User Stores**

Typically, you configure Privileged Access Manager to use the groups and users that are defined in the enterprise user stores. When you create an access rule that references an enterprise user or group, or when a user logs in to the operating system, Privileged Access Manager creates a record in its database for that user or group.

These records have the class `XUSER` (for enterprise users) or `XGROUP` (for enterprise groups). They hold the properties that Privileged Access Manager requires to enforce access rules. You do not need to manage them, because Privileged Access Manager creates them as required.

The only properties of an enterprise user or group that CA Access Control fetches from the enterprise user stores are the names and the group membership properties.

## **Guidelines for Managing Accessors in Enterprise Stores**

If you decide to manage your accessors in enterprise user stores, consider the following guidelines.

### **Users and Groups That Must Be Defined in the Database**

Privileged Access Manager needs some users and groups to be defined in its database, rather than in the enterprise user stores. These include:

- Predefined users
- Predefined groups
- Privileged Access Manager administrator
- Profile groups
- Logical users

### **Restrictions on the Use of Enterprise Users**

Privileged Access Manager imposes the following restrictions on the use of enterprise users:

- You cannot create, or cannot refer to, an enterprise user in Privileged Access Manager if it has the same name as a user defined in the database.
- You cannot create, delete, or modify an enterprise user using the selang AC environment.
- You cannot use an enterprise user as a logical user.
- By default, you cannot create an enterprise user in Privileged Access Manager unless the user is already defined in the enterprise user store. However, you can enable or disable this behavior on UNIX systems.

## **Restrictions on the Use of Enterprise Groups**

Privileged Access Manager imposes the following restrictions on the use of enterprise groups:

- You cannot create or delete an enterprise group within the selang AC environment.
- You cannot change the membership of an enterprise group within the selang AC environment.
- You cannot use an enterprise group as a Profile Group.

## **Enable or Disable the Use of Enterprise Users and Groups**

By default, Privileged Access Manager does not use the groups and users who are defined in the enterprise user stores. We recommend that you enable this feature. Only if you need compatibility with previous versions of Privileged Access Manager, disable this feature by setting `osuser_enabled` to "no".

### **Example: Enable the Use of Enterprise Users and Groups on Windows**

The following registry setting enables the use of enterprise users and groups on Windows:

Key: HKLM\SOFTWARE\ComputerAssociates\AccessControl\OS\_user

Name: `osuser_enabled`

Type: REG\_DWORD

Value: yes

### **Example: Enable the Use of Enterprise Users and Groups on UNIX**

The following commands stop Privileged Access Manager, enable the use of enterprise users and groups on UNIX, and restart Privileged Access Manager:

```
secons -s

seini -s OS_User.osuser_enabled yes

seload
```

## **Enable or Disable the Creation of XUSER Records at Enterprise User Login**

If Privileged Access Manager is enabled to use enterprise users, by default it creates a record (in the XUSER class) for a user when that user logs in. Sometimes you do not want this, for example, if thousands of users log on at the same time each day.

To prevent Privileged Access Manager creating XUSER records when users log in, change the value of the configuration setting `create_user_in_db` to 0 (zero). To re-enable this behavior, set the value to 1 (one).

### **Example: Disable the Automatic Creation of XUSER Records on Enterprise User Login on Windows**

The following registry setting disables the automatic creation of an enterprise user record in Privileged Access Manager on Windows:

- Key: HKLM\Software\ComputerAssociates\AccessControl\OS\_user
- Name: `create_user_in_db`
- Type: REG\_DWORD
- Value: 0

### **Example: Disable the Automatic Creation of XUSER Records on Enterprise User Login on UNIX**



The following commands stop Privileged Access Manager, disable the automatic creation of a XUSER record on UNIX, and restart Privileged Access Manager:

```
secons -s

seini -s OS_User.create_user_in_db 0

seload
```

### **Enable or Disable Checking Enterprise Store Before Creating XUSER Records on UNIX**

Sometimes you may want to create an enterprise user in Privileged Access Manager when the user is not defined in the enterprise user store. On Windows, you cannot create an enterprise user in Privileged Access Manager unless the user exists in the Windows user store. On UNIX, the default behavior is the opposite to Windows. However, on UNIX, you can enable or disable this default behavior.

To disable checking (and therefore allow Privileged Access Manager to create XUSER records when there is no enterprise user equivalent), change the value of the configuration setting `verify_osuser` to 0. To enforce checking, set the value to 1.

#### **Example: Enable Creation of XUSER Records without Checking the Enterprise User Store**

The following set of commands stops Privileged Access Manager, enables the creation of XUSER records with no enterprise store equivalents, and restarts Privileged Access Manager:

```
secons -s

seini -s OS_User.verify_osuser 0

seload
```

### **Recycled Enterprise Store Accounts on Windows**

*Recycled accounts* are enterprise store users or groups that have been deleted and recreated. For example, a user resigns and you remove the user from the user store, and later you create another account with the same name.

Recycled accounts are a security concern because you do not want new accessors to have the same access permissions as the old account with the same name. To solve this problem, Privileged Access Manager authorization is based on the SID. When you create an accessor, it does not automatically receive the permissions of a deleted accessor with the same name.

#### **WARNING**

Recycled account accessors *do not* inherit the old access permissions. However, database access rules, which mention the accessor name (not SID), make it seem like these rules still apply. Use the `secons -checkSID` command to resolve this issue.

### **Resolve Recycled Enterprise Accounts on Windows**

If an enterprise account (user or group) with associated database rules is recycled (deleted and created with the same name), the old database rules appear to apply to the new account. However, as Privileged Access Manager authorization is based on SID, these rules no longer apply, and you must create rules for the new group. Before you can create the rules, you have to resolve recycled accounts.

**Follow these steps:**

1. Open a command prompt and run the following commands:

```
secons -checkSID -users
```

```
secons -checkSID -groups
```

Privileged Access Manager works through all the enterprise user accounts it has (XUSER records) and then all the group accounts (XGROUP records) and identifies accounts with an SID that differs from the SID of the enterprise account. It renames these accounts in Privileged Access Manager using the following naming convention: *SID (accountName)*

2. Create the rules for the recycled account.

**Note:** Recycled user accounts are resolved in this way when the user logs in or tries to access a resource. We recommend that you run the `secons -checkSID` command as a scheduled task when you create an enterprise account.

**Example: A Recycled Group Account**

Company ABCD has a group that is called *interns* in its enterprise store. The group has nine members and they are working on productA. The administrator makes the group that is known to Privileged Access Manager and assigns it with access permissions to the files group members must access, as follows:

```
nxg interns owner(msmith)
```

```
auth file c:\products\productA\materials\* xgid(interns) access(all)
```

```
auth file c:\HR\interns\* xgid(interns) access(read)
```

When the interns complete their tenure with ABCD, the enterprise store administrator deletes the group. Three months later, a new group of interns with six members is created in the enterprise store, with the same name. The old rules in the Privileged Access Manager database still exist so it seems like the new *interns* group inherited the permissions of the old group. However, these rules apply to the old interns group and the Privileged Access Manager administrator must create rules for the new group.

To do this, the administrator has to identify and resolve the recycled interns account, as follows:

```
secons -checkSID -groups interns
```

This renames the XGROUP resource, and any access rules references to it, to "*SID (domain\interns)*". Now, the administrator can create rules for the new interns group that works on productB:

```
nxg interns owner(msmith)
```

```
auth file c:\products\productB\materials\* xgid(interns) access(all)
```

```
auth file c:\HR\interns\* xgid(interns) access(read)
```

## Database Accessors

No matter how you manage your users, define some accessors in the product database, as described in the following sections.

### Predefined Users

Privileged Access Manager predefines the following users, which you cannot delete:

- **+devcalc**  
(Windows) The user name under which Privileged Access Manager runs the deviation calculation process, devcalc.
- **\_dms**  
Installed on the advanced policy management server components' databases (DMS, DH reader, and DH writer), the \_dms user is used by policyfetcher and devcalc to communicate with the DH and DMS.
- **nobody**  
The nobody user is a user record that cannot correspond to a real user. Use this record to create rules that do not give the associated permissions to any user. For example, you can set *nobody* as the owner of resources, meaning that no user gets the permissions associated with owning that record.
- **+reportagent**  
The user name under which Privileged Access Manager runs the Report Agent.
- **\_seagent**  
\_seagent is the user name under which Privileged Access Manager runs some internal processes, such as:
  - The PMDB process, sepmdd
  - (UNIX) The deviation calculation process, devcalc
  - The user and group record update exit processes
 The \_seagent user has the SERVER attribute.
- **\_sebuildla**  
(UNIX) The \_sebuildla user is the user name under which Privileged Access Manager runs the sebuildla utility to create a lookaside database for the Privileged Access Manager Control daemon, seosd.
- **\_seoswd**  
(UNIX) \_seoswd is the user name that is used to run the seoswd watchdog daemon to monitor the file information and digital signatures of programs that are defined in the database as trusted programs.
- **\_undefined**  
\_undefined represents all users that are undefined in Privileged Access Manager. You can use \_undefined to include undefined users in ACLs.

### Predefined Groups

Privileged Access Manager comes with predefined groups. Except for the \_interactive and \_network groups, you add users to these groups in the same way as you do for any other group.

- **\_abspath**  
If a user is in the \_abspath group when logging in, that user must use absolute path names to invoke programs.
- **\_interactive**  
A user is a member of the \_interactive group only for the purposes of an access attempt. Users are members of the \_interactive group if they are logged into the same host as the resource they are trying to access. Privileged Access Manager dynamically and automatically manages the membership of the \_interactive group; you cannot change the membership.
- **interactive\_restricted**  
The users in the interactive\_restricted group need strong authentication before they can modify files. Users in the Interactive\_restricted group can read files and can execute commands. They cannot modify any files except for a

predefined list of non-files that they are authorized to modify. A message reminds users to run the sepromote utility to authenticate when they must remove the restriction.

- **\_network**

This is the complementary group to \_interactive. A user is a member of the \_network group for the purposes of access only. Users are members of the \_network group if they are trying to access a resource from a different host than the resource belongs to. Privileged Access Manager dynamically and automatically manages the membership of the \_network group; you cannot change the membership.

- **\_restricted**

For users in the \_restricted group, all files, and on Windows registry keys too, are protected by Privileged Access Manager. If a file or a Windows registry key does not have an access rule that is explicitly defined, access permissions are covered by the \_default record for that class (FILE or REGKEY).

**Note:** Users in the \_restricted group may not have sufficient authorization to do their work. If you plan to add users to the \_restricted group, consider using Warning mode initially.

- **\_surrogate**

When a user uses a member of the \_surrogate group as a surrogate, Privileged Access Manager writes a full trace in the audit trail of the surrogate's actions, tagged with the original user's name.

### Example: Adding a User to the \_restricted Group Using selang

The following selang command adds the enterprise user john\_smith to the \_restricted group:

```
joinx john_smith group(_restricted)
```

## Profile Groups

A *profile group* is a group that is defined in the product database that contains default values for user properties. When you assign a user to a profile group, the profile group provides those values to the user unless they have already been set for the user.

You can specify a profile group for a user when you create the user, or you can assign the user to the profile group afterwards.

Profile groups let administrators efficiently create a standard setup with specific permissions for any new user who is assigned to that group. This setup can specify such things as the home directory of the user, the audit properties, the PMDB that defines the access authorities, and various password rules affecting a user who is associated with a profile group.

### How the Product Uses Profile Groups to Determine User Properties

The following process describes how the product uses profile groups to determine user properties:

1. The product checks if the user's record in the USER or XUSER class has a value for the property. If the user's record has a value for the property, then the product uses that value.
2. The product checks if the user is assigned to a profile group. If the user is assigned to a profile group, the process continues. If the user is not assigned to a profile group, then the product assigns the default property value to the user.
3. The product checks if the profile group has a value for that property. If the profile group has a value for the property, The product assigns that value to the user. If the profile group does not have a value for the property, The product assigns the default property value to the user.

**Note:** If the audit property of a user or profile group is not set, the audit property of a group can affect the audit property of a user.



## Accessor Management

You can create, modify, and delete database or enterprise user or group records by using Privileged Access Manager Endpoint Management or by using selang.

## Manage Users or Groups

If you want to view or modify the properties of a particular accessor, or if you want to delete an accessor, you must first find that accessor.

### To manage users or groups

1. In Privileged Access Manager Endpoint Management, do as follows:
  - a. Click Users.
  - b. Click either the Users or Groups subtab.
 Depending on your selection, the Users or the Groups page appears.
2. Complete the following fields in the Search section:
  - **User/Group Name**  
Defines a mask for the accessors you want to find. You can enter the full name of the accessor you are after or you can use a mask. For example, use \*admin\* to list accessors whose name contains "admin". Use an \* (asterisk) to list all accessors and a ? (question mark) to replace a single character.
  - **User/Group Repository**  
Specifies the source from which you want to fetch a list of accessors. The source can be either:
    - a. **Internal Accounts** - accessors that are defined in the database
    - b. **Enterprise Accounts** - accessors that are defined in specific enterprise user stores
  - **Show only AC accounts/profiles**  
Specifies whether to list only those accounts that have records in the Privileged Access Manager database as follows:
    - a. If you chose Internal Accounts, the application lists only those accounts that exist in the database (no native accounts).
    - b. If you chose Enterprise Accounts, the application lists only those accounts that have a Privileged Access Manager enterprise profile (XUSER or XGROUP records).
3. Click Go.  
A list of accessors that exist in the repository you chose appears.
4. Do *one* of the following:
  - Click  in the View column to view the properties of the accessor.
  - Click  in the Delete column to delete the accessor.
  - Click the name of the accessor to modify the properties of the accessor.
  - Select the accessors that you want to delete and click Delete.
  - Click Create User or Create Group to create a user or group record in the product database.

### Example: Search for Enterprise Users in a Repository

The following graphic shows you the result of looking for all users in the ABC-DM1 enterprise user store.

**Search** **Create User**

**Required**

**User Name:**  For multiple entities please use the wildcard \*

**User:**  **Go**

**Repository:**

**Options:** ☐ Show only AC accounts/profiles

**User Environment**

- With AC Profile

- Without AC Profile

---

**Users list for: COMP001** **Create User**

Here are the results for XUSER with name: \* at 08/07/09 00:22

Select and: **Delete** 1 - 10 of 12 > >>

| Select                   | Env. | Name                  | Comment | View | Delete |
|--------------------------|------|-----------------------|---------|------|--------|
| <input type="checkbox"/> |      | ABC-DM1\ac_ent_pers   |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\Administrator |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\alice         |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\ASPNET        |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\bob           |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\entmgmt       |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\Guest         |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\IUSR_IIS_SVR1 |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\IWAM_IIS_SVR1 |         |      |        |
| <input type="checkbox"/> |      | ABC-DM1\rand          |         |      |        |

1 - 10 of 12 > >>

Total of 12 objects.

## User Management Using Selang

Use the following selang commands for records of enterprise users:

- **newxusr** and **editxusr** - define a new enterprise user record
- **chxusr** and **editxusr** - change the properties of an enterprise user
- **find xuser** - list enterprise users that have a Privileged Access Manager record
- **rmxusr** - delete a user
- **show xuser** - display the properties of an enterprise user

Use the following selang commands for Privileged Access Manager database user records:

- **newusr** and **editusr** - define a new user record
- **chusr** and **editusr** - change the properties of a user
- **rmusr** - delete a user
- **find user** - list database users
- **show user** - display the properties of a user

### Example: Define a User in the Database Using selang

The following selang command defines a new user in the Privileged Access Manager database with security level 100:

```
newusr internalUser level(100)
```

### Example: Change a Property of an Enterprise User Using selang

The following selang command gives the AUDITOR property to an enterprise user Terry:

```
chxusr Terry auditor
```

## Group Management Using selang

You can change any property of any group, except that you cannot change the name or the membership of enterprise groups (from within Privileged Access Manager).

To change group properties or to assign access rights associated with groups, you can use Privileged Access Manager Endpoint Management Console or the following `selang` commands:

- **join[-]** and **joinx[-]**  
Change the membership of an internal group  
Use `join` to add internal accessors to the group. Use `joinx` to add enterprise groups and users to an internal group. Use the `-` (minus) form of the commands to remove accessors.
- **editgrp**, **newgrp**, **chgrp**  
Change the non-membership properties of an internal group
- **editxgrp**, **newxgrp**, **chxgrp**  
Change the non-membership properties of an enterprise group
- **rmgrp**, **rmxgrp**  
Remove a user group

#### Example: Define a Group in the Database Using `selang`

The following `selang` command defines a new group `sales` in the database. The full name of the group is `Sales Department`:

```
newgrp sales name('Sales Department')
```

#### Example: Change a Property of a Group Defined in the Database Using `selang`

The following `selang` command makes Privileged Access Manager audit all events for members of the group `AC_admins`:

```
chgrp AC_admins audit(all)
```

#### Example: Add an Enterprise Group to an ACL Using `selang`

The following `selang` command adds the enterprise group `mygroup` to the ACL of the `myfile`:

```
Authorize FILE (myfile) xgid(mygroup)
```

#### Example: Add an Enterprise User to a Group Defined in the Database Using `selang`

The following `selang` command adds the enterprise user `mydomain\administrator` to the group `AC_admins` which is defined in the database:

```
joinx mydomain\administrator group(AC_admins)
```

#### Example: Add an Enterprise Group to a Group Defined in the Database Using `selang`

The following `selang` command adds the enterprise group `Guests` to the `_restricted` group:

```
joinx Guests group(_restricted)
```

## Classes

In Privileged Access Manager, the *class* of a record defines the properties that the record can have. All records in a class have the same properties, though different values for these properties.

Examples of classes are:

- **TERMINAL** class - This class contains records for terminals, such as `tty1`, `tty`.
- **FILE** class - This class contains records for files.
- **PROGRAM** class - This class contains records of programs.

Each record contains values for the properties appropriate to the record class. For example, a record in the `XUSER` class includes such properties as the location and working hours of the enterprise user. A record in the `HOSTNET` class includes such properties as net services and IP address data.

Privileged Access Manager includes predefined classes. You can also define new classes, named user-defined classes. This article describes a default record for class and new user-defined classes.

### Default Record for Class

Most classes can include a default record (`_default`) specifying access types for resources of that class that are not defined in database records of their own.

Like other resource records, the `_default` record can include an ACL and a `defaccess` field. You can create a `_default` record for all classes except `USER`, `GROUP`, `CATEGORY`, `SECLABEL`, and `SEOS`.

### UACC Class (Deprecated)

The UACC class is no longer recommended. To specify the default values for records in a class, use the `_default` record.

Some earlier versions of Privileged Access Manager used a separate class, called UACC, for records resembling the `_default` records of other classes. The UACC class is no longer recommended, and if you use a `_default` record, the equivalent record in the UACC class is not checked. In future versions, the UACC class may no longer be supported.

For example, suppose user Henderson tries to kill process `store_log`. Privileged Access Manager checks for authorization in the following order. The primary question is this: Is the process `store_log` defined in the database? Privileged Access Manager searches the database for a record that is named `store_log` in the `PROCESS` class.

- If no such record can be found, the process is not defined to Privileged Access Manager. In that case, the product uses either the `_default` record of class `PROCESS`, or the `PROCESS` record in the UACC class, to determine whether Henderson is allowed to kill `store_log`.
  - If user Henderson appears in the `_default` record's ACL, the authority specified in it is applied.
  - If Henderson does *not* appear in the `_default` record's ACL, the authority specified in the `defaccess` property of the `_default` record is applied. This authority is applied to all users who do not appear explicitly in the `_default` ACL.
- If process `store_log` is defined in the database, then the question is whether user Henderson appears in the ACL for process `store_log` in the database.
  - If user Henderson appears in the ACL for process `store_log`, the authority specified there is applied.
  - If Henderson does *not* appear in the ACL, Privileged Access Manager applies the authority specified in the default access property of the `store_log` resource. This authority is called the resource's default access.

**Note:** If the default access (`defaccess`) of `_default` is set to `NONE`, or if `_default` is not specified and the default of the corresponding resource in the UACC class is `NONE`, then any accessor attempting to access a resource not defined in the class is denied access to the resource.

**Note:** If the default access of `_default` (or UACC) is set to the highest authority (`ALL`, or in some cases `READ` or `EXECUTE`), then any resource that is not explicitly protected is accessible to everyone.

### Predefined Classes

The predefined classes can be categorized into the following types:

| Class Type   | Purpose                                                                                |
|--------------|----------------------------------------------------------------------------------------|
| Accessor     | Defines objects that access resources, such as users and groups.                       |
| Definition   | Defines objects that define security entities, such as security labels and categories. |
| Installation | Defines objects that control the behavior of Privileged Access Manager.                |
| Resource     | Defines objects that are protected by access rules.                                    |



The following table contains a list of all predefined classes.

| Class      | Class Type | Description                                                                                                                                                                                                                                  |
|------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ADMIN      | Definition | Lets you delegate administrative responsibilities to users who do not have the ADMIN attribute. You give these users global authorization attributes and limit their administration authority scope.                                         |
| AGENT      | Resource   | Not applicable                                                                                                                                                                                                                               |
| AGENT_TYPE | Resource   | Not applicable                                                                                                                                                                                                                               |
| APPL       | Resource   | Not applicable                                                                                                                                                                                                                               |
| AUTHHOST   | Accessor   | Not applicable                                                                                                                                                                                                                               |
| CATEGORY   | Definition | Lets you define a security category.                                                                                                                                                                                                         |
| CONNECT    | Resource   | Lets you protect outgoing connections. The records in this class define which users can access which Internet hosts.<br><br>Before you activate the CONNECT class, be sure that the streams module is active.                                |
| CONTAINER  | Resource   | Lets you define a group of objects from other resource classes, thus simplifying the job of defining access rules when a rule applies to several different classes of objects.                                                               |
| FILE       | Resource   | Lets you protect a file, a directory, or a file name mask.                                                                                                                                                                                   |
| GAPPL      | Resource   | Not applicable                                                                                                                                                                                                                               |
| GAUTHHOST  | Definition | Not applicable                                                                                                                                                                                                                               |
| GFILE      | Resource   | Each record in this class defines a group of files or directories. Grouping is accomplished by explicitly connecting files or directories (resources of the FILE class) to the GFILE resource in the same way users are connected to groups. |
| GHOST      | Resource   | Each record in this class defines a group of hosts. Grouping is accomplished by explicitly connecting hosts (resources of the HOST class) to the GHOST resource in the same way users are connected to groups.                               |
| GROUP      | Accessor   | Each record in this class defines an internal group.                                                                                                                                                                                         |
| GSUDO      | Resource   | Each record in this class defines a group of commands that one user can execute as if another user were executing it. The sesudo command uses this class.                                                                                    |
| GTERMINAL  | Resource   | Each record in this class defines a group of terminals.                                                                                                                                                                                      |

|               |            |                                                                                                                                                                                                                                                                                                          |
|---------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HNODE         | Definition | The HNODE class contains information about the organization's Privileged Access Manager hosts. Each record in the class represents a node in the enterprise.                                                                                                                                             |
| HOLIDAY       | Definition | Each record in this class defines one or more periods when users need extra permission to log in.                                                                                                                                                                                                        |
| HOST          | Resource   | Each record in this class defines a host. The host is identified by either its name or its IP address. The object contains access rules that determine whether the local host can receive services from this host.<br><br>Before you activate the HOST class, be sure that the streams module is active. |
| HOSTNET       | Resource   | Each record in this class is identified by an IP address mask and contains access rules.                                                                                                                                                                                                                 |
| HOSTNP        | Resource   | Each record in this class defines a group of hosts, where the hosts belonging to the group all have the same name pattern. Each HOSTNP object's name contains a wildcard.                                                                                                                                |
| LOGINAPPL     | Definition | Each record in the LOGINAPPL class defines a login application, identifies who can use the program to log in, and controls the way the login program is used.                                                                                                                                            |
| MFTERMINAL    | Definition | Each record in the MFTERMINAL class defines a Mainframe Privileged Access Manager administration computer.                                                                                                                                                                                               |
| POLICY        | Resource   | Each record in the POLICY class defines the information required to deploy and remove a policy. It includes a link to the RULESET objects that contain a list of the selang commands for deploying and removing the policy.                                                                              |
| PROCESS       | Resource   | Each record in this class defines an executable file.                                                                                                                                                                                                                                                    |
| PROGRAM       | Resource   | Each record in this class defines a trusted program that can be used with conditional access rules. Trusted programs are setuid/setgid programs that are monitored by the Watchdog to ensure they are not tampered with.                                                                                 |
| PWPOLICY      | Definition | Each record in the PWPOLICY class defines a password policy.                                                                                                                                                                                                                                             |
| RESOURCE_DESC | Definition | Not applicable                                                                                                                                                                                                                                                                                           |
| RESPONSE_TAB  | Definition | Not applicable                                                                                                                                                                                                                                                                                           |

|            |              |                                                                                                                                                                                                                                                                                                                                                              |
|------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULESET    | Resource     | Each record in the RULESET class represents a set of rules which defines a policy.                                                                                                                                                                                                                                                                           |
| SECFILE    | Definition   | Each record in this class defines a file that must not be altered.                                                                                                                                                                                                                                                                                           |
| SECLABEL   | Definition   | Each record in this class defines a security label.                                                                                                                                                                                                                                                                                                          |
| SEOS       | Installation | The one record in this class specifies your active classes and password rules.                                                                                                                                                                                                                                                                               |
| SPECIALPGM | Installation | Each record in the SPECIALPGM class registers backup, DCM, PBF and PBN functions in Windows or xdm, backup, mail, DCM, PBF, and PBN programs in UNIX or associates an application that needs special authorization protection with a logical user ID. This allows you to set access permissions according to what is being done rather than who is doing it. |
| SUDO       | Resource     | This class, used by the sesudo command, defines commands that one user (such as a regular user) can execute as if another user (such as root) were executing them.                                                                                                                                                                                           |
| SURROGATE  | Resource     | Each record in this class contains access rules for an accessor that define who can use that accessor as a surrogate.                                                                                                                                                                                                                                        |
| TCP        | Resource     | Each record in this class defines a TCP/IP service, for example, mail or http or ftp.                                                                                                                                                                                                                                                                        |
| TERMINAL   | Resource     | Each record in this class defines a terminal-a device from which a user can log in.                                                                                                                                                                                                                                                                          |
| UACC       | Resource     | Defines default access rules for each resource class.                                                                                                                                                                                                                                                                                                        |
| USER       | Accessor     | Each record in this class defines an internal user.                                                                                                                                                                                                                                                                                                          |
| USER_ATTR  | Definition   | Not applicable                                                                                                                                                                                                                                                                                                                                               |
| USER_DIR   | Resource     | Not applicable                                                                                                                                                                                                                                                                                                                                               |
| XGROUP     | Accessor     | Each record in this class defines an enterprise group to Privileged Access Manager.                                                                                                                                                                                                                                                                          |
| XUSER      | Accessor     | Each record in this class defines an enterprise user to Privileged Access Manager.                                                                                                                                                                                                                                                                           |

**Note:** Privileged Access Manager database classes TCP and SURROGATE are not active by default.

If you upgrade from an earlier release where the TCP class is active but you do not have any TCP records and have not changed the \_default TCP resource, Privileged Access Manager deactivates the class during upgrade. The same is true for the SURROGATE class.

**Note:** If you upgrade from an earlier release where the SURROGATE class is active and you have defined SURROGATE records or have changed the value of any SURROGATE record from its default, Privileged Access Manager retains the SURROGATE class configuration after the upgrade. The class remains active and kernel mode interception remains enabled.

**Note:** For more information about Privileged Access Manager classes, see the *selang Reference section*.

## **User-Defined Classes**

Privileged Access Manager enables you to define new classes, so that you can protect abstract objects by creating appropriate records for them.

### **Example: User-Defined Class for a Database View**

A site may use a database to store and display proprietary data.

You can define a user-defined class DATABASE\_VIEWS, and can define each database view to be a resource member of that class. Give the resource an ACL that defines the access authority that is required to create that database view. When a user attempts to create a database view, Privileged Access Manager checks the access authority of the user, and permits or disallows the creation based on the ACL.

### **Wildcards in User-Defined Classes Resources**

By using wildcards in the name of a resource in a user-defined class, you can create a resource record that corresponds to multiple physical resources: any physical resource with a name that matches the wildcard pattern is protected by the access authorities associated with the resource record.

Following are the wildcards that you can use:

- \* for any number of any characters
- ? for any one character

If a physical resource name matches more than one resource record name, the longest non-wildcard match is used for that resource.

Privileged Access Manager does *not* accept the following wildcard patterns as resource names:

- \*
- /\*
- /tmp/\*
- /etc/\*

### **User-Defined Class Example**

Suppose that your system serves a bank and you want to protect transfers of large amounts between accounts. You can use the following outline to set up this security.

1. Define a class to contain the records that describe transfers, named, for example, TRANSFERS.
2. For each monetary level transfer that you want to protect, define a record in the TRANSFERS class.  
For example, you might define records that are named Upto.\$1K, Upto.\$1M, Upto.\$10M, and Over.\$10M.  
Define any other resources to control transfers as members of the TRANSFERS class.
3. To give different users permission to perform different maximum transfers, grant or deny them access to the various records in the TRANSFERS class.
4. In addition, to handle programmatic transfers, insert in the bank's money-transfer program a call to the Privileged Access Manager API. This call checks the permission of the user before it allows a transfer to proceed.

## Windows Services Protection

### NOTE

The rules that are created using the selang CLI are not displayed properly in the Endpoint Management UI. The display name is shown incorrectly in the UI. You can edit the display name to the correct service name. Do not use the Endpoint Management UI to browse for the services, since the UI shows the display name of the service instead of the service name. If you want to use the UI to create the rule, ensure that you specify the correct name for the service.

Privileged Access Manager lets you protect Windows services. A *Windows service* is a program that runs in the background on Windows. A Windows Service is the Windows equivalent to a daemon on UNIX.

The Privileged Access Manager Windows service protection intercepts service access events that originate from one of the following sources:

- Service management and information events  
Privileged Access Manager intercepts the services.exe process for each service access. This includes starting or stopping a service. For example, net start *service* and net stop *service* are protected. Intercepted events in this case are audited using the name of the protected service.
- Service database management events  
Privileged Access Manager intercepts registry calls to the service control management database to protect against service state queries or changes. This means that the product automatically protects the registry areas that are associated with the protected service. Effectively, Privileged Access Manager protects the following registry keys when you define service protection:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\service_name
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\service_name
```

Intercepted events in this case are audited using the full registry path.

You protect a Windows service in the same way as you protect other resources. You assign a resource to the service and add accessors to the access control lists of the resource. The resource class for a Windows service is WINSERVICE. A WINSERVICE resource has two access control lists: an ACL and an NACL. Valid access types for an entry in a WINSERVICE access control list are:

- Read
- Modify
- Start
- Stop
- Pause
- Resume

### WARNING

Windows 2012, Windows 2012 R2, and Windows 2016 do not support the GID and UID attributes that are associated with logical groups and users, respectively. So, these attributes that were supported in Windows 2008 R2 and earlier are no longer supported from this release.

This article contains the following sections:

### Review Considerations

Consider the following points if the endpoint operating system is Windows 2012, Windows 2012 R2, or Windows 2016:

- The rules that are created to protect the Windows services do not apply to the critical services such as eventlog and dnscient.
- Rules that are created for third-party services work only if those services are not controlled by any security product/suite other than Privileged Access Manager. Else, conflict between Privileged Access Manager and other security product/suite can result in an undefined behavior of Privileged Access Manager. To avoid this issue, ensure that no other security suite products are installed on the host that has Privileged Access Manager installed.
- To modify the startup type of a non-critical Windows service, the rule must contain both the Start and Modify permissions. However, the sc utility lets you update the startup type of a service even if the rule is created with only the Modify permission. By default, the sc utility provides the Start permission.
- A rule that is created for a service can include auditing. In such cases, when you run the seaudit utility, the audit results are displayed with a delay of few seconds as all the Windows event logs must be scanned. Wait until the results are displayed before you rerun the utility.
- If a service has an active rule, do not delete the Windows event logs that are available under Security. If you want to delete the Security-related Windows event logs, delete the rule and then delete those event logs.
- Rules can be applied only to those users who are part of the administrators group.

### **Enable and Disable Windows Services Protection**

You can enable or disable the Privileged Access Manager protection of Windows services.

To enable protection of Windows services, set the configuration setting OperationMode in the Instrumentation\PlugIns\WinServiceplg section of the Privileged Access Manager registry to 1. To disable protection, set OperationMode to 0.

By default, Privileged Access Manager enables protection of Windows services.

For Privileged Access Manager to protect a Windows service, enable protection and ensure that the WINSERVICE class is active.

### **Protect a Windows Service**

You can protect a Windows Service and so provide extra protection to Windows operations.

#### **Follow these steps:**

1. Ensure that you have [enabled Windows services protection](#).
2. Ensure that the WINSERVICE class is active. (It is active by default.)
3. Create a WINSERVICE record in Privileged Access Manager, with the same name as the Windows service you want to protect.

**Note:** The Windows service name is shown on the General tab of the Windows service properties dialog. However, the Windows service name is not the same as the "display name" on that tab.

4. Assign the accessors and their access authorization to the service.  
The service is now protected.

### **Example: Restrict Access to the Print Spooler**

On Windows, the print spooler has the service name spooler. The following selang commands ensure that the WINSERVICE class is active and sets the default access to the spooler to *read*.

```
setoptions class+(WINSERVICE)

editres WINSERVICE(spooler) defacc(R)
```

### **Example: Authorize users of a group to access the Spooler service**

You can create a group and provide access to a Windows service to the members of that group.

**Follow these steps:**

1. Create a native user using the following command:  

```
nu <hostname>\testuser password(XXX) nt
```
2. Create a logical group without an owner using the following command:  

```
ng <hostname>\xgroup owner(nobody) nt
```
3. Associate the group that was created with the database using the following command:  

```
nxg <hostname>\xgroup
```
4. Associate the user with the group using the following command:  

```
join <hostname>\testuser group(<hostname>\testgroup) nt
```
5. Enable the Spooler service with default access set to no user using the following command:  

```
er winservice spooler owner(nobody) defacc(n)
```
6. Authorize the group's users to access the Spooler service, using the following command:  

```
auth winservice spooler XGID(<hostname>\xgroup) access(start,stop,r)
```

**Non-IPv4 Telnet Connections Are Not Secured on Windows Server 2008**

On Windows Server 2008, Privileged Access Manager cannot secure a telnet connection unless it uses IPv4.

To protect a localhost telnet connection from the localhost to the localhost on Windows Server 2008, modify the /etc/HOSTS file as follows:

```
127.0.0.1      localhost

#           ::1          localhost

127.0.0.1##    <your server name without domain suffix>
```

If your computer is on an IPv6 domain, add the following line:

```
127.0.0.1    <your server name with domain suffix>
```

**View Access Attempts to a Protected Windows Service**

When Privileged Access Manager protects a Windows service, it intercepts, and records in the audit log, access attempts that are related to the service. These access attempts can be a result of using the services.exe process to manage the service (start, stop, and so on). They can also be the result of registry access to the service database management area of the protected service. While the former access is audit contains only the service name, the latter (registry access) contains the full registry path. To view all access attempts related to a Windows service, use wildcards.

To view access attempts to a protected Windows service, create an audit filter that filters audit records of class WINSERVICE and resource name *\*myService\**

Privileged Access Manager displays all audit records for the WINSERVICE resource you defined (whether access was attempted through the registry or through a service management interface).

**WARNING**

Seaudit log entries for WinService class interception are created in the Japanese and Korean environments only if the audit parameter is explicitly specified in the rule.

**Example: View All Access Attempts to the Print Spooler Service**

This example assumes that you defined the Print Spooler service to Privileged Access Manager with no access as follows:

```
er winservice spooler defaccess(none) owner(nobody) audit(all)
```

where audit can have the following values:

- **All**  
Displays all logs including success and failure attempts
- **None**  
No logs are displayed
- **S**  
Displays only the successful attempts
- **F**  
Displays only the failure attempts

You can then use the seaudit utility to list all access attempts to the Print Spooler service as follows:

```
seaudit -resource WINSERVICE *spooler* *
```

This command lists all audit records for the class WINSERVICE that were recorded for access attempts to the Print Spooler service. The resulting output can look as follows:

```
seaudit - Audit log lister
03 Apr YYYY 16:53:48 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:53:48 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:53:50 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:53:50 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:53:53 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:53:53 D WINSERVICE    bigHost1\Administrator Read      69  2 Spooler
    c:\WINDOWS\system32\services.exe bigHost1.comp.com
03 Apr YYYY 16:54:10 D WINSERVICE    bigHost1\Administrator Read      69  2 HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Services\Spooler
    C:\WINDOWS\regedit.exe bigHost1.comp.com
03 Apr YYYY 16:54:10 D WINSERVICE    bigHost1\Administrator Read      69  2 HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Services\Spooler
    C:\WINDOWS\regedit.exe bigHost1.comp.com
03 Apr YYYY 16:54:19 D WINSERVICE    bigHost1\Administrator Read      69  2 HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Services\Spooler
    C:\WINDOWS\regedit.exe bigHost1.comp.com
03 Apr YYYY 16:54:26 D WINSERVICE    bigHost1\Administrator Read      69## 2 HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Services\Spooler
    C:\WINDOWS\regedit.exe bigHost1.comp.com
03 Apr YYYY 16:54:26 D WINSERVICE    bigHost1\Administrator Modify    69  2 HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Services\Spooler
    C:\WINDOWS\regedit.exe bigHost1.comp.com
```

Total records displayed 11



## Windows Registry Protection

Privileged Access Manager lets you protect entries in the Windows registry.

You provide protection to a registry key by assigning a resource of class REGKEY to the key. You can then specify access authorities on the key, as with other resources.

Specifying access rights on a key does not affect access to subkeys of the key, except for enumeration (listing) of subkeys. Enumeration of subkeys requires read access to the key.

Privileged Access Manager only supports the REGVAL resource in the AC environment on Windows Server 2003 and subsequent Windows systems. On these systems, Privileged Access Manager protects registry values with the REGVAL class. The REGKEY access authorization does not affect access to the values of the key.

On earlier systems, Privileged Access Manager does not support the REGVAL resource in the AC environment. The access authorization that is applied on a REGKEY record does affect access to the values of the key.

REGKEY and REGVAL records have identical structures. Each record contains the following access control lists:

- ACL
- CALACL
- NACL
- PACL

REGVAL and REGKEY records both allow the same access types, which are as follows:

- READ
- WRITE
- DELETE
- NONE

### NOTE

Privileged Access Manager registry protection does not protect the registry operations of loading and unloading a hive. On Windows Server 2008 and subsequent systems, Privileged Access Manager returns a value of REG\_NONE if an accessor tries to access a protected registry value with access NONE. A value of REG\_NONE confirms that a value is present but does not specify the value.

## Protect a Windows Registry Entry

You can protect a Windows registry entry, and so provide extra protection to Windows operations.

### To protect a Windows registry entry:

1. If you want to use the REGKEY and REGVAL class records, ensure that these classes are active. (They are active by default.)
2. Create a REGKEY or a REGVAL record with the name of the registry key or value you want to protect.

### NOTE

Use the full registry path name to specify the key or value. You can use a wildcard to specify all subkeys or subkey values that are nested under a key.

The registry entry is now protected with the default access that Privileged Access Manager provides for the record.

3. (Optional) Assign the users and groups, with their access authorization, to the appropriate access control list in the REGKEY or REGVAL record.

### Example: Provide default access of NONE to a Registry Key

The following selang command provides default access of NONE to a registry key:

```
er REGKEY HKEY_LOCAL_MACHINE\SOFTWARE\Test\Key1 defacc(NONE) owner(nobody)
```

As a result, the default access to key1 is as follows:

| Action                                   | Systems earlier than Windows Server 2003 | Windows Server 2003 systems and later | Windows Server 2008 systems and later |
|------------------------------------------|------------------------------------------|---------------------------------------|---------------------------------------|
| Enumerate subkeys                        | Deny                                     | Deny                                  | Deny                                  |
| Query, modify, rename, or delete key     | Deny                                     | Deny                                  | Deny                                  |
| Load or unload hive to key               | Deny                                     | Deny                                  | Deny                                  |
| Enumerate values                         | Deny                                     | Deny                                  | Permit                                |
| Read, create, rename, or delete values   | Deny                                     | Permit                                | Permit                                |
| Enumerate subkeys of subkeys             | Deny                                     | Permit                                | Permit                                |
| Create subkeys                           | Permit                                   | Permit                                | Permit                                |
| Query, modify, rename, or delete subkeys | Permit                                   | Permit                                | Permit                                |
| Load or unload hive to subkeys           | Permit                                   | Permit                                | Permit                                |

#### Example: Provide default access of READ to a Registry Key

The following selang command provides default READ access to a registry key:

```
er REGKEY HKEY_LOCAL_MACHINE\SOFTWARE\Test\Key1 defacc(READ) owner(nobody)
```

As a result, the default access to Key 1 is as follows:

| Action                                   | Systems earlier than Windows Server 2003 | Windows Server 2003 and later | Windows Server 2008 and later |
|------------------------------------------|------------------------------------------|-------------------------------|-------------------------------|
| Enumerate subkeys                        | Permit                                   | Permit                        | Permit                        |
| Read key                                 | Permit                                   | Permit                        | Permit                        |
| Modify, rename, or delete key            | Deny                                     | Deny                          | Deny                          |
| Load or unload hive to key               | Deny                                     | Deny                          | Deny                          |
| Enumerate values                         | Permit                                   | Permit                        | Permit                        |
| Read values                              | Permit                                   | Permit                        | Permit                        |
| Create, rename, or delete values         | Deny                                     | Permit                        | Permit                        |
| Enumerate subkeys of subkeys             | Permit                                   | Permit                        | Permit                        |
| Create subkeys                           | Permit                                   | Permit                        | Permit                        |
| Query, modify, rename, or delete subkeys | Permit                                   | Permit                        | Permit                        |
| Load or unload hive to subkeys           | Permit                                   | Permit                        | Permit                        |
| Enumerate subkey values                  | Permit                                   | Permit                        | Permit                        |
| Create subkey values                     | Permit                                   | Permit                        | Permit                        |

#### Example: Provide default access of NONE to a Registry Key Wildcard

The following selang command provides default access of NONE to all subkeys in a registry key:

```
er REGKEY HKEY_LOCAL_MACHINE\SOFTWARE\Test\Key1\* defacc(NONE) owner(nobody)
```

The wildcard (\*) does not apply to Key1, but to all subkeys of Key1. This rule means that any form of access is denied to all subkeys of Key1. Access is also denied to rename or delete Key1, due to the parent protection rule.

This command permits access to the values of Key1. The access to values of subkeys of Key1 (for example, values of Key1\subkey1\ ) varies between different Windows systems:

- On Windows Server 2003 and subsequent systems, this command denies access to enumerate the values of any subkey of key1. However, the command grants access to create, rename, delete, and read the values.
- On systems earlier than Windows Server 2003, this command denies all access to the values of subkeys of Key1.

### Example: Provide default access of NONE to a Registry Value

The following selang command protects a specific registry value with access NONE on Windows Server 2003 and subsequent systems:

```
er REGVAL HKEY_LOCAL_MACHINE\SOFTWARE\TestKey\value1 defacc(NONE) owner(nobody)
```

#### NOTE

On Windows Server 2008 and subsequent systems, Privileged Access Manager returns a value of REG\_NONE if an accessor tries to access a protected registry value with access NONE. A value of REG\_NONE confirms that a value is present but does not specify the value.

## Protect File Streams

A stream is a sequence of bytes. File streams contain file data, and provide additional information about a file. For example, you can create a stream that contains keywords or metadata.

#### NOTE

File streams are only available on the NTFS file system. For more information on file streams, see the Microsoft Developer Network (MSDN) Library website.

When you create a FILE rule, Privileged Access Manager automatically protects the default data stream for the file. For example, a rule that protects the file c:\foo.txt also governs permissions to c:\foo.txt::\$DATA. However, Privileged Access Manager does not automatically protect any non-default data streams. Create extra file protection rules for these data streams.

To protect file streams, do either *one* of the following procedures:

- To protect a specific stream, create a file rule in the format:  
drive:\path\filename.ext:stream
- To protect a specific stream type of a particular stream, create a file rule in the format:  
drive:\path\filename.ext:stream:type
- To protect all streams, create a generic file rule in the format:  
drive:\path\filename.ext:\*

### Example: Protect All File Streams

The following selang command creates a generic file rule that protects all the streams in the file c:\foo.txt:

```
er file c:\foo.txt:* owner(nobody) defaccess(none)
```

### Example: Protect a Specific Stream

The following selang command creates a file rule that protects the stream *mystream* in the file c:\foo.txt:

```
er file c:\foo.txt:mystream owner(nobody) defaccess(none)
```

## Internal File Protection (Windows)

During installation, Privileged Access Manager writes rules to protect two types of internal files:

- Internal rules: Protect configuration files, log files, and database files.  
You cannot delete internal rules.
- Default rules: Protect sensitive files such as root and server certificates that you use to encrypt and authenticate communication.  
You can delete default rules after installation.

### Internal File Rules

Internal file rules protect configuration files, log files, and database files. Internal file rules are not visible in selang and cannot be deleted. However, you can write FILE rules to override the internal file rules. If you delete these FILE rules, Privileged Access Manager reverts to the internal file rules.

Except for database files, files that the product protects with internal file rules have the following access rights:

- Full access for Privileged Access Manager internal processes
- Read and execute (where relevant) access for all other accessors

Database files that the product protects with internal file rules have the following access rights:

- Privileged Access Manager internal processes have full access to the database.
- The NT AUTHORITY\System user has read access to the database.
- All other accessors have no access to the database.

#### NOTE

The default access rights for all other accessors were changed in r12.5 SP3. In previous releases, all other accessors had read access by default to the database files.

Privileged Access Manager protects the following files with internal file rules. The second column of the table lists the registry subkey and entry that specifies the file location, where applicable. Privileged Access Manager creates its registry entries under the following registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl

#### NOTE

Some file locations are defined internally and do not have a corresponding registry entry. You cannot configure the location of these files.

| File                 | Registry Subkey and Entry | Default File Location                      |
|----------------------|---------------------------|--------------------------------------------|
| seosdrv.sys          | -                         | %SystemRoot%\system32\drivers\seosdrv.sys  |
| cainstrm.sys         | -                         | %SystemRoot%\system32\drivers\cainstrm.sys |
| drveng.sys           | -                         | %SystemRoot%\system32\drivers\drveng.sys   |
| pwdchange.dll        | -                         | %SystemRoot%\system32\pwdchange.dll        |
| SUSRAUTH.dll         | -                         | %SystemRoot%\system32\SUSRAUTH.dll         |
| eACSubAuth.dll       | -                         | %SystemRoot%\system32\eACSubAuth.dll       |
| eACPasswordFiltr.dll | -                         | %SystemRoot%\system32\eACPasswordFiltr.dll |
| All database files   | SeOSD\dbdir               | ACInstallDir\Data\seosdb                   |

|                   |                            |                        |
|-------------------|----------------------------|------------------------|
| All help files    | lang\help_path             | ACInstallDir\Data\help |
| All binaries      | -                          | ACInstallDir\bin       |
| seosd.trace       | SeOSD\trace_file           | ACInstallDir\log       |
| seos.audit        | logmgr\audit_log           | ACInstallDir\log       |
| seos.audit.bak    | logmgr\audit_back          | ACInstallDir\log       |
| seos.error        | logmgr\error_log           | ACInstallDir\log       |
| seos.error.bak    | logmgr\error_back          | ACInstallDir\log       |
| seos.msg          | message\filename           | ACInstallDir\Data      |
| stop.ini          | STOP\STOPIniFileName       | ACInstallDir\Data      |
| stopsignature.dat | STOP\STOPSignatureFileName | ACInstallDir\Data      |
| response.ini      | SeOSD\ResponseFile         | ACInstallDir\Data      |
| audit.cfg         | logmgr\AuditFiltersFile    | ACInstallDir\Data      |

Privileged Access Manager creates the following registry keys during installation and protects them with internal file rules under REGKEY, REGVAL class:

**Under HKLM\SYSTEM\\*ControlSet\*\Services:**

- CA Access Control Agent Manager
- CA Access Control Report Agent
- CA Access Control Web Service
- SeOS Agent
- SeOS Engine
- SeOS Policy Model(DH\_\_)
- SeOS Policy Model(DH\_\_WRITER)
- SeOS Policy Model(DMS\_\_)
- SeOS TD
- SeOS Watchdog
- cainstrm
- driveng
- seosdrv

**Under HKLM\SYSTEM\\*ControlSet\*\Enum\Root:**

- LEGACY\_CAINSTRM
- LEGACY\_DRVENG
- LEGACY\_SEOSDRV

**NOTE**

For more information about configuration settings, see the *Reference Guide*.

**Default File Rules**

Privileged Access Manager creates default file rules during installation to protect sensitive files. Default file rules are visible in selang and can be deleted.

The following table lists the sensitive files that the product protects with default file rules, and the access rights and permitted accessors for the files.

In the table, *PMDBDir* is the directory in which the policy model databases (PMDBs) reside, and *pmd\_name* is the name of each policy model. By default, *PMDBDir* is located at *ACInstallDir\Data*. The location of *PMDBDir* is defined in the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\_Pmd_directory_
```

| File                                          | Default Access | Permitted Accessors |
|-----------------------------------------------|----------------|---------------------|
| <i>ACInstallDir\data\crypto\crypto.dat</i>    | None           | sechkey             |
| <i>ACInstallDir\data\crypto\def_root.pem*</i> | None           | sechkey             |
| <i>ACInstallDir\data\crypto\sub.key</i>       | None           | sechkey             |
| <i>ACInstallDir\data\crypto\sub.pem</i>       | None           | sechkey             |
| <i>ACInstallDir\log\policyfetcher.log</i>     | Read           | +policyfetcher      |
| <i>PMDBDir\pmd_name</i>                       | Read, Chdir    | -                   |
| <i>PMDBDir\pmd_name\*</i>                     | Read, Execute  | -                   |

## Manage PAM SC Authorization

### Access Authorities

The main purpose of Privileged Access Manager is to assign and enforce access authorities, also known as access rights.

An access authority always has the following components:

- The resource that the access applies to, for example, a file, host, or terminal
- The type of access, for example, read, write, delete, log in, run
- The accessor, which is either a user or a group

A user has the authority to access a resource in a certain way because one or more of the following circumstances are true:

- The user has the access authority, as granted by the resource ACL
- The user is a member of a group that has access authority.
- The user is running a program that has the access authority. For example, the user has the authority to run a program in the SPECIALPGM class, or to run a command in the SUDO class.

#### NOTE

For more information about access authority by class, see the *selang Reference Guide*.

### Setting Access Authority - Examples

#### Example: Give an internal User Read Access

The following *selang* command adds the internal user *internal\_user* to the ACL of terminal *tty30*, to give read access to the terminal:

```
authorize TERMINAL tty30 access(READ) uid(internal_user)
```

#### Example: Give an Enterprise User Read Access

The following *selang* command adds the enterprise user *Terry* to the ACL of terminal *tty30*, to give read access to the terminal:

```
authorize TERMINAL tty30 access(READ) xuid(Terry)
```

**Example: Change an Access Authority of an Enterprise User to a Resource**

The following selang command sets Terry's access to terminal tty30 to none, and so denies Terry access:

```
authorize TERMINAL tty30 access(NONE) xuid(Terry)
```

**Example: Remove the Access Authority of an Enterprise User from a Resource**

The following selang command removes Terry from the ACL in the terminal tty30:

```
authorize- TERMINAL tty30 xuid(Terry) access-
```

Terry now has the default access to the terminal.

**Example: Give an Enterprise User Sub-administrator Access**

The following selang commands set up the enterprise user Terry as a sub-administrator with the authority to manage users and files:

```
authorize ADMIN USER xuid(Terry)
authorize ADMIN FILE xuid(Terry)
```

**Access Control Lists**

The access authorities to a resource are specified in an access control list. Every resource record has at least two access control lists:

- **ACL**  
Specifies the accessors that are granted access to the resource, together with the type of access that they are granted.
- **NACL**  
Specifies the accessors that are denied authorization to the resource, together with the type of access that they are denied.

The access authority can also depend on the circumstances around the access, such as whether the user is logged in locally or not.

***Conditional Access Control Lists***

Conditional Access Control Lists (CACLS) provide an extension to ACLs. When an accessor attempts to access a resource, if the resource's ACL and NACL do not define an access authority for the user, Privileged Access Manager examines the conditional access control lists.

The conditional access control lists specify access to resource where the access is by a particular method, for example by using a specified program.

For example you can use a conditional access control list to define a program pathing rule.

Privileged Access Manager allows the following conditional access control lists:

- Program Access Control Lists (PACLs)
- TCP class access control lists
- CALENDAR class access control lists

To define an entry in a conditional access control list entry, you can use the `via` option of the selang `authorize` command.

In common with other access control lists, each entry in a conditional access control list specifies the accessors that are granted access to the resource, together with the type of access that they are granted. In addition, an entry in a conditional access control list specifies the condition under which the authority is assigned. For a PACL, the condition is the name of a program which the accessor needs to run to have the access.

**Example: Using a PACL**

To allow the enterprise user sysadm1 to become superuser only by running the program secured\_su, you can specify the corresponding conditional access rule using the following selang command:

```
authorize SURROGATE user.root xuid(sysadm1) via(pgm(secured_su))
```

### **defaccess The Default Access Field**

The record for a resource can include a default access field, defaccess. The value of the defaccess field specifies the access authority that is allowed to accessors who are not covered by any of the resource access control lists.

### **How Access Authority to a Resource Is Determined**

When an accessor attempts to access a resource, Privileged Access Manager checks the access authority. The product runs one or more checks in a predetermined order, until it gets a result. If any check produces an access result (deny or allow access), Privileged Access Manager does not check any further. Instead, the product returns the result.

The order in which it runs through these checks is important. For each resource, Privileged Access Manager checks the access records in the following order by default:

1. The time-based restrictions of the resource
2. The ownership of the resource (owners are allowed access)
3. B1 checks
4. The NACL of the resource
5. The ACL of the resource
6. The PACL of the resource
7. The defaccess field of the resource

The setting of the accpac option determines the order of the last two checks. You can disable the use of resource PACL by using the selang command setoptions setpacl-.

#### **NOTE**

One access control list can contain more than one entry that affects a user. For example, it can contain an entry that mentions a user explicitly, and also entries for each of the groups to which the user belongs. Privileged Access Manager checks all the possible entries at each level before it goes to the next level. For more information about how it resolves conflicting rules at each level, see Interaction Between User and Group Access Authorities.

### **Example: The Resultant Permission on a File**

For the following table, assume that an accessor named user1 attempts to read the resource file1.

In the following table Privileged Access Manager is following the default setting of the accpac option to use the PACL.

| Entry in NACL for user1 | Entry in ACL for user1 | Entry in PACL for user1 | Entry in defaccess | Resulting Permission                          |
|-------------------------|------------------------|-------------------------|--------------------|-----------------------------------------------|
| Read                    | (Any)                  | (Any)                   | (Any)              | Read denied                                   |
| (Not defined)           | None                   | (Any)                   | (Any)              | Read denied                                   |
| (Not defined)           | Read                   | (Any)                   | (Any)              | Read granted                                  |
| (Not defined)           | (Not defined)          | via pgm securereader    | (Any)              | Read allowed through the securereader program |
| (Not defined)           | (Not defined)          | (Not defined)           | Read               | Read granted                                  |

Where an entry is shown as *(Not defined)*, no entry for user1 exists in that access control list.

Where an entry is shown as *(Any)*, the entry in that access control list does not matter, because Privileged Access Manager does not check it.



The order that Privileged Access Manager checks is from left to right. Notice that for all rows, the cells to the right of a cell with a defined access have the value *(any)*. Conversely all the cells to the left of a cell that contains a defined access have the value *(not defined)*.

### **Interaction Between User and Group Access Authorities**

You can explicitly grant or deny access authorities to a user, and also to groups to which the user belongs. Sometimes these can conflict. The following example shows what results if conflicting access authorities are assigned to the same resource when a user is a member of two groups (Group 1 and Group 2).

It assumes that the accumulative group rights option is set (the default setting).

| Access Authority for User | Access Authority for Group 1 | Access Authority for Group 2 | Resulting Access Authority |
|---------------------------|------------------------------|------------------------------|----------------------------|
| Access denied             | <i>(Any)</i>                 | <i>(Any)</i>                 | Access denied              |
| Access granted            | <i>(Any)</i>                 | <i>(Any)</i>                 | Access granted             |
| <i>(Not defined)</i>      | Access granted               | <i>(Not defined)</i>         | Access granted             |
| <i>(Not defined)</i>      | <i>(Not defined)</i>         | Access granted               | Access granted             |
| <i>(Not defined)</i>      | Access granted               | Access granted               | Access granted             |
| <i>(Not defined)</i>      | Access denied                | <i>(Any)</i>                 | Access denied              |
| <i>(Not defined)</i>      | <i>(Any)</i>                 | Access denied                | Access denied              |

Where an entry is shown as *(Not defined)*, this means that no entry for the user or group is defined.

Where an entry is shown as *(Any)*, this means that the access authority does not matter, because Privileged Access Manager does not check it.

### **Accumulative Group Rights (ACCGRR)**

The *accumulative group rights* option (ACCGRR) affects how Privileged Access Manager checks the ACL of the resource. If ACCGRR is enabled, Privileged Access Manager checks the ACL for the authorities that are granted from all the groups to which the user belongs. If ACCGRR is disabled, Privileged Access Manager checks the ACL to see if any of the applicable entries contain the value none. If so, access is denied. Otherwise Privileged Access Manager ignores all group entries except the first applicable one in the access control list. By default the option is enabled.

To enable the ACCGRR option, you can use the following `selang` command:

```
setoptions accgrr
```

To disable the ACCGRR option, you can use the following `selang` command:

```
setoptions accgrr-
```

### **Security Levels, Categories, and Labels**

Security levels and security categories provide additional ways to restrict access to a resource, complementary to the use of access control lists.

Security labels are a means to bundle security levels and categories together, to manage them more easily.

#### **Security Levels**

A *security level* is an integer between 0 and 255 that you can assign to accessors and resources. An accessor cannot access a resource if the accessor has a security level less than the security level assigned to the resource, even if the user is granted access authority in the resource's access control list. If a resource has a zero security level, security level checking is not checked for that resource.

An accessor with a security level of zero cannot access any resource that has a non-zero security level.

### **Security Categories**

A *security category* is the name of record in the CATEGORY class. You can assign a security category to accessors and to resources. An accessor can access a resource only if the accessor is assigned to all of the security categories assigned to the resource.

### **Security Labels**

A *security label* is the name of a record in the SECLABEL class. A security label bundles together a security level and a set of security categories. Assigning a security label to an accessor or a resource gives the accessor or resource the combined security level and security categories associated with the security label. A security label overrides any specific security level and category assignments in an accessor or resource.

#### **Example: Use of a Security Label High\_Security**

Assume High\_Security is a security label that contains a security level 255 and the security categories MANAGEMENT and CONFIDENTIAL.

If you assign a user user1 to the security label High\_Security, user1 has a security level of 255 and also has the security categories MANAGEMENT and CONFIDENTIAL.

## **User Impersonation Protection**

When you enable the SURROGATE class in Privileged Access Manager, you enable user impersonation protection. User impersonation protection lets you specify that a user or group can only change their SID (security identifier) to another SID if a specific rule permits the change. This protection prevents a user from impersonating the identity of another user if they are not authorized to do so.

### **NOTE**

A security identifier is a numeric value that identifies a user or group to the operating system.

For example, you define a Privileged Access Manager rule that prevents any user from impersonating Administrator. User Tom tries to run a program that performs some tasks as Administrator. Privileged Access Manager does not permit the program to execute because Tom does not have permission to impersonate Administrator.

You can run user impersonation protection in two modes:

- User mode interception
- Kernel mode interception

### **User Mode Interception**

If you enable user mode interception, Privileged Access Manager intercepts only the impersonation requests that originate from the Windows RunAs utility. User mode interception is available on all supported Windows versions.

### **NOTE**

User mode interception is enabled by default when you enable user impersonation protection: that is, when you enable the SURROGATE class.

The advantages of user mode interception include:

- Privileged Access Manager identifies the user who made the original impersonation request.  
In many Windows applications, including the RunAs utility, the NT AUTHORITY\SYSTEM user impersonates the requesting user and makes the impersonation request. User mode interception identifies the user executing the utility, not the NT AUTHORITY\SYSTEM user who makes the request. For example, if Tom executes RunAs to impersonate

Administrator, the NT AUTHORITY\SYSTEM user makes the impersonation request. Privileged Access Manager identifies Tom as the requesting user.

- Privileged Access Manager intercepts impersonation requests only when a user executes the RunAs utility. This process minimizes performance impact.

A disadvantage of user mode interception is that Privileged Access Manager does not intercept every impersonation request from every Windows process.

### **Kernel Mode Interception**

If you enable kernel mode interception, Privileged Access Manager intercepts every impersonation request from all Windows processes. Kernel mode interception is not available on all supported Windows versions.

#### **NOTE**

For more information about the Windows versions for which kernel mode interception is not available, see the *Release Notes*.

An advantage of kernel mode interception is that it lets you protect every impersonation request that is made on a Windows computer.

The disadvantages of kernel mode interception include:

- If the NT AUTHORITY\SYSTEM user impersonates the requesting user and makes the impersonation request, Privileged Access Manager does not identify the user who made the original impersonation request. For example, RunAs, ftp, and telnet requests are all made by the NT AUTHORITY\SYSTEM user. If Tom executes RunAs to impersonate Administrator, the NT AUTHORITY\SYSTEM user makes the impersonation request. Privileged Access Manager identifies NT AUTHORITY\SYSTEM as the requesting user.
- Privileged Access Manager intercepts every impersonation request that the OS makes as part of its normal operation, which can have a performance impact. Although Privileged Access Manager caches impersonation requests, the authorization engine must still authorize many impersonation events.

### **How Privileged Access Manager Responds to User Impersonation Requests**

Each record in the SURROGATE class defines restrictions that protect a user from impersonation attempts. Privileged Access Manager treats an impersonation request as an abstract object that only authorized users can access. A record in the SURROGATE class represents each user or group who has surrogate (impersonation) protection.

When a user or group makes a request to impersonate another user or group, Privileged Access Manager follows these steps:

1. Checks the access authority of the SURROGATE record for the user or group. Depending on the SURROGATE record, *one* of the following happens:
  - The SURROGATE record for the user or group specifically permits or denies the impersonation. Privileged Access Manager uses the access authority of the SURROGATE record to permit or deny the impersonation request.
  - The user or group does not have a SURROGATE record. The process goes to Step 2.
2. Checks the access authority of the default SURROGATE record for the user or group, as follows:
  - If the requester is a user, Privileged Access Manager gives the user the access type that is defined in the USER.\_default SURROGATE record.
  - If the requester is a group, Privileged Access Manager gives the user the access type that is defined in the GROUP.\_default SURROGATE record.

**NOTE**

The default access authority of the USER.\_default, GROUP.\_default, and \_default SURROGATE records are read. This means that Privileged Access Manager permits any request to impersonate a user or group, unless a SURROGATE record for the user or group prohibits the impersonation request. To change this behavior, change the access authority of the USER.\_default and GROUP.\_default records. You can also set the same default for users and groups by changing the access authority of the \_default SURROGATE record.

**Enable User Impersonation Protection**

User impersonation protection lets you set rules to permit or deny requests to impersonate specific users and groups.

**To enable user impersonation protection**

1. (Optional) Enable kernel mode interception, as follows:

- a. Stop Privileged Access Manager.

- b. Change the value of the following registry value to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\
SeOSD\SurrogateInterceptionMode
```

- c. Restart Privileged Access Manager.

**NOTE**

User mode interception is enabled by default.

2. Open a selang command prompt window.

3. Enable the SURROGATE class:

```
setoptions class+(SURROGATE)
```

4. Define selang rules for SURROGATE records for your Privileged Access Manager implementation.

5. (Kernel mode interception only) Define a rule that lets the SYSTEM user impersonate the user that makes the impersonation request:

```
auth SURROGATE USER.Administrator uid("NT AUTHORITY\SYSTEM") acc(R)
```

Windows identifies many utilities and services (for example, Run As) as user "NT AUTHORITY\SYSTEM" and not as the user running the utility. Define a rule for the SYSTEM user to let users who run these utilities impersonate another user.

**Example: Permit Any Impersonation Request**

The following selang rule lets any user impersonate another user, unless a record in the database explicitly prevents the impersonation:

```
editres SURROGATE _default defaccess(READ)
```

**Example: Prevent Impersonation of a Specific User**

The following selang rule prevents any user impersonating Administrator, unless a record in the database explicitly permits the user impersonation:

```
newres SURROGATE USER.Administrator defaccess(NONE)
```

**Example: Permit a Group to Impersonate a User**

The following rule permits members of the Administrators group to impersonate Administrator:

```
authorize SURROGATE USER.Administrator gid("Administrators")
```

## Set Up the Surrogate DO Facility

Operators, production personnel, and end users must often perform tasks that only the superuser can perform.

The traditional solution is to supply all these users with the password of the superuser, which compromises the security of the site. The secure alternative, keeping the password secret, results in the system administrator being overloaded with legitimate requests from users to perform routine tasks.

The Surrogate DO (`sesudo`) utility solves this problem. The utility allows users to perform actions that are defined in the SUDO class, where each record contains a script. The utility specifies which users and groups can run the script, and it lends them the necessary permissions for the purpose.

For example, to define a SUDO resource that starts the "Print Spooler" service as if the user were System, enter the following `selang` command:

```
newres SUDO StartSpooler data("net start spooler")
```

This `newres` command defines `StartSpooler` as a protected action that some users may receive System authority to perform.

### WARNING

In the data property, use a full absolute path name. A relative path name could accidentally execute a Trojan horse program that is planted in an unprotected directory.

In addition, users can be authorized to perform the `StartSpooler` action by using the `authorize` command. For example, to allow the user *operator1* to start the "Print Spooler" service, enter the following `selang` command:

```
authorize SUDO StartSpooler uid(operator1)
```

You can also explicitly prevent a user from performing the protected action by using the `authorize` command. For example, to prevent the user *operator2* from starting the "Print Spooler" service, enter the `selang` command:

```
authorize SUDO StartSpooler uid(operator2) access(None)
```

Executing the `sesudo` utility performs the protected action. For example, the user *operator1* would start the "Print Spooler" service using the following command:

```
sesudo -do StartSpooler
```

The `sesudo` utility first checks whether the user is authorized to perform the SUDO action. If the user is authorized to the resource, the utility executes the command script defined in the resource. In the example, `sesudo` checks whether *operator1* is authorized to perform the `StartSpooler` action. The utility then invokes the command "net start spooler" with System credentials.

### NOTE

For more information about the `sesudo` utility, see the *Reference Guide*.

## Define SUDO Records (Task Delegation)

A record in the SUDO class stores a command script so that users can run the script with borrowed permissions. The SUDO record controls the ability to borrow permissions, as does the `sesudo` command that executes the scripts.

### NOTE

If you create a SUDO record for an interactive Windows application, set the interactive flag for the SUDO record. If you do not set the interactive flag, the application runs in the background and you cannot interact with it. For more information, see the *Troubleshooting Guide*.

In a SUDO record, the comment property is used for a special purpose. This property is often known by its alternate name: the data property.

The value of the comment property is the command script, with the optional addition of one or more script parameter values that are to be prohibited or permitted. The entire comment property value must be enclosed in single quotes. Reference executables by their complete path names to prevent Trojan horses from taking their place.

The comment property has this format:

```
comment('cmd[;[prohibited-values][;permitted-values]]')
```

Because the lists of prohibited and permitted values are optional, a simple comment property value can be the following:

```
newres SUDO NET comment('net use')
```

The simple value in the command means that the command `sesudoNET` executes the command `'net use'`. No particular script parameter values are prohibited; all are permitted.

Wildcards and powerful variables give you flexibility in specifying prohibited and permitted parameters. The wildcards that you can use are the standard Windows wildcards. Prohibited and permitted parameters can also contain the following variables:

| Variable | Description                                                                                  |
|----------|----------------------------------------------------------------------------------------------|
| \$A      | An alpha value                                                                               |
| \$G      | An existing Privileged Access Manager group name                                             |
| \$H      | (UNIX only) A parameter that starts with the home directory of the user                      |
| \$N      | A numeric value                                                                              |
| \$O      | The Privileged Access Manager name of the user running <code>sesudo</code>                   |
| \$U      | An existing Privileged Access Manager user name                                              |
| \$e      | An empty entry.<br>Use this entry to specify a SUDO command with no parameters for the rule. |
| \$f      | An existing file name                                                                        |
| \$g      | An existing Windows group name                                                               |
| \$h      | An existing host name                                                                        |
| \$r      | An existing file with Windows read access                                                    |
| \$u      | An existing Windows user name                                                                |
| \$w      | An existing file with Windows write access                                                   |
| \$x      | An existing file with Windows execute access                                                 |

If you append a list of the prohibited parameter values to the script:

- Separate the script from the prohibited parameter values with a semicolon, but keep them all inside the single quotes. For example, if you want to prevent the user from using `-start` but you permit the user to use all other parameters, enter the following command:

```
newres SUDO scriptname comment('cmd;-start')
```

where *cmd* represents your script.

Alternatively, if you do not allow any parameter values, but you want all parameters defaulted, define the SUDO record as follows:

```
newres SUDO scriptname comment('cmd;*')
```

- If a script parameter has more than one prohibited value, use the space character as a separator. For example, if you want to prevent the user from using `-start` and `-stop` but you permit the user to use all other parameters, enter the following command:

```
newres SUDO scriptname comment('cmd;-start -stop')
```

- If more than one script parameter has prohibited values, use the pipe character (|) as a separator between sets of prohibited values. For example, if you want to prevent the user from using -start and -stop for the script's first parameter, and from using any existing Windows user name for the second parameter (see the previous list of variables), enter the following command:

```
newres SUDO scriptname comment('cmd;-start -stop | $u')
```

If the script has more parameters than you list, then your last set of prohibited parameters applies to all the remaining parameters.

If you append a list of the permitted parameter values to the script,

- The sesudo utility checks that the parameter values:
  - Do *not* match any of the corresponding *prohibited* values.
  - Match at least one of the corresponding *permitted* values.

This means that if a parameter value is in the prohibited list, it is not permitted even if it is also specified in the permitted list.

Separate the list of *permitted* values from the list of *prohibited* values with a semicolon, but keep them all inside the single quotes. Even if you have no list of prohibited values, you still need the semicolon. Otherwise, what you intend to permit is prohibited. For example, if you want to allow only the value NAME as a parameter value for the script, enter the following command:

```
newres SUDO scriptname comment('cmd;;NAME')
```

- Just as in the other list,
  - If a script parameter has more than one permitted value, use the space character as a separator.
  - If more than one script parameter has permitted values, use the pipe character (|) as a separator between sets of permitted values.

For example, if you have two parameters, and the first must be numeric but must not be a Windows user name, and the second must be alphabetic but must not be a Windows group name, enter the following command:

```
newres SUDO scriptname comment('cmd;$u | $g ;$N | $A')
```

If the script has more parameters than you list, then your last set of permitted parameters applies to all the remaining parameters.

Thus, the overall format for the comment property is this: first the script; then the prohibited values, parameter by parameter; then the permitted values, parameter by parameter:

```
comment('cmd; \
param1_prohib1 param1_prohib2 ... param1_prohibN | \
param2_prohib1 param2_prohib2 ... param2_prohibN | \
...
paramN_prohib1 paramN_prohib2 ... paramN_prohibN ; \
param1_permit1 param1_permit2 ... param1_permitN | \
param2_permit1 param2_permit2 ... param2_permitN | \
...
paramN_permit1 paramN_permit2 ... paramN_permitN')
```

The sesudo utility checks each parameter that the user enters in the following manner:

1. Test if parameter N matches permitted parameter N. (If permitted parameter N does not exist, the last permitted parameter is used.)
2. Test if parameter N matches prohibited parameter N. (If prohibited parameter N does not exist, the last prohibited parameter is used.)

If all the parameters match permitted parameters, and none match prohibited parameters, sesudo executes the command.

**Example: Set Up Task Delegation that Permits a User to Run net send**

The following procedure shows you how you let user Takashi execute the net send command and prevent him from executing the net start command:

1. In Privileged Access Manager Endpoint Management click the Users tab, then click the Authorization and Delegation subtab.  
The Authorization and Delegation menu options appear on the left.
2. Click Task Delegations.  
The Task Delegations page appears.
3. Click Create Task.  
The Create Task page appears.
4. Complete the dialog fields as follows:

| Field                | Value                           |
|----------------------|---------------------------------|
| Name                 | NET                             |
| Data                 | net;start;send *                |
| Owner                | nobody                          |
| Default Access       | None (option cleared)           |
| Authorized Accessors | USER: Takashi<br>Allow: Execute |

1. 1. 1. Click Save.  
The new task delegation (SUDO) record is created.
2. Test the task delegation rule:
  - a. Log in as Takashi.
  - b. Open the command prompt and execute the following:

```
sesudo -do NET start
```

```
sesudo: you are not allowed to use 'start' as parameter number 1.
sesudo: you are not allowed to use 'start' as parameter number 1.
sesudo -do NET send comp message
sesudo -do NET send comp message
```

The following message appears:

#### NOTE

*net start* does not execute because it was defined as a prohibited value.

3. Execute the following value: NET send
4. The command executes.

### Example: Authorize a User to Execute Privileged Operations using an Interactive Application

A user can perform highly privileged operations using any snap-in MSC module, as the following example shows:

1. In Privileged Access Manager Endpoint Management click the Users tab, then click the Authorization and Delegation subtab.  
The Authorization and Delegation menu options appear on the left.
2. Click Task Delegations.  
The Task Delegations page appears.
3. Click Create Task.  
The Create Task page appears.



## 4. Complete the dialog fields as follows:

| Field                | Value                         |
|----------------------|-------------------------------|
| Name                 | services                      |
| Data                 | c:\winnt\system32\mmc.exe     |
| Owner                | nobody                        |
| Options              | Interactive (option selected) |
| Default Access       | None (option cleared)         |
| Authorized Accessors | USER: Tori<br>Allow: Execute  |

## 1. Click Save.

The new task delegation (SUDO) record is created. The Interactive option provides the desktop user interface that can be used by whoever is logged in when the service is started. This is available only if the service is running as a LocalSystem account.

## 2. Test the task delegation rule:

- a. Log in as Tori.
- b. Open the command prompt and execute the following:

```
sesudo -do services
```

- a. mmc.exe will start.

## Check User Inactivity

The inactivity feature protects the system from unauthorized access through accounts whose owners are away or no longer employed by the organization. An inactive day is a day in which the user does not log in. You can specify the number of inactive days that must pass before the user account is suspended and cannot log in. Once an account is suspended, you must manually reactivate it.

### NOTE

Password changes count as activities, in terms of inactivity checks. If a user's password changes, that user cannot become suspended due to inactivity.

You can set the number of inactive days with the inactive property of a USER class record or a GROUP class record. The latter affects only users that have that group as a profile group. You can also set inactivity for all users systemwide with the INACT property of the SEOS class.

In selang, use the following command to specify inactivity globally:

```
setoptions inactive (numdays)
```

To set the number of days for a group (which overrides the systemwide inactive setting for that group), use the following command:

```
editgrp groupName inactive (numdays)
```

To set the number of days for a user (which overrides group and systemwide settings for that user), use the following command:

```
editusr userName inactive (numdays)
```

To reactivate a suspended user account, use the following command:

```
editusr userName resume
```

To reactivate a suspended profile group, use the following command:

```
editgrp userName resume
```

To disable inactive login checking at the systemwide level, use the following command:

```
setoptions inactive-
```

To disable inactive login checking for a group, use the following command:

```
editgrp groupName inactive-
```

To disable inactive login checking for a user, use the following command:

```
editusr userName inactive-
```

## Security Auditors

One of the most important tasks of security auditors and system administrators is auditing or monitoring system activity to detect suspicious or malicious activity. Security auditing plays an essential role in a secure environment, and the security auditing features in Privileged Access Manager include the following:

- Providing a reliable indication of who has accessed the system, what resources have been accessed, how the resource has been accessed (for example, read a file), and when resources have been accessed
- Notifying and alerting appropriate users in case of an attempted security breach, even if the attempt failed
- Indicating what changes have been made to the security rules, and by whom
- Providing a means to test the effect of access rules before they are enforced

Privileged Access Manager auditing is modeled after real-world auditing: security auditors act independently of system and security administrators, although you can change your implementation so that this is not the case if some other model is more appropriate for your environment.

A security auditor is a user to whom the AUDITOR attribute is assigned. Users defined as security auditors are permitted to perform auditing tasks such as changing the audit rules that are assigned to users and resources. They are also authorized to use the Privileged Access Manager auditing utilities without being required to have the ADMIN attribute.

## Events Interception

Privileged Access Manager intercepts an event if the following two conditions are met:

- The appropriate class is active.
- A rule anticipating this event exists in the database.

For example, you can use the following generic rule to audit all file accesses to files that reside in c:\data\payroll:

```
newres FILE c:\data\payroll\*
```

Ensure that the FILE class is active (the default).

## Types of Intercepted Events

Privileged Access Manager intercepts two types of events:

- Interception Events  
Information from an interception event is cached as part of the process for future use by an audit event.
- Audit Events

## **Interception Modes**

Based on the interception mode, Privileged Access Manager intercepts, checks for authorization, and logs audit records of access request events. Privileged Access Manager has the following modes of interception:

- Full Enforcement mode
- Audit Only mode
- No Interception mode

### **NOTE**

Warning mode is not an interception mode. Warning mode works in Full Enforcement mode only and is designed for short-term use during implementation.

## **Audit Only Mode**

*Audit Only mode* records all intercepted events without checking or enforcing access rules. Use this mode to collect data for compliance requirements or regulations. In Audit Only mode, Privileged Access Manager intercepts the event and writes an audit event but does not process the request for authorization and does not enforce rules. As a result, Privileged Access Manager permits all access requests that it intercepts. This means that the authorization result recorded in the audit log for all events is *P* (permitted).

The following restrictions apply to Audit Only mode: The audit properties of the resource and the user are *not* considered. Audit Only mode records *all intercepted* events regardless of resource- or user-specific settings.

## **Set Up Audit Only Mode**

*Audit Only mode* records all intercepted events without checking or enforcing access rules. Use this mode to collect data for compliance requirements or regulations.

To set up Audit Only mode, set the SeOSD\GeneralInterceptionMode Privileged Access Manager registry entry to 1.

### **WARNING**

If you use Audit Only mode, ensure that you have enough disk space for the audit logs and that the size limit of the audit log is large enough. Also consider options for [audit log backup](#).

## **Warning Mode**

*Warning Mode* is a property that you can apply to a resource, and an option that you can apply to a class. If Warning mode is applied to a resource or a class and an access violates an access rule, Privileged Access Manager writes an audit log entry with the return code W. However, the product permits the access to the resource. If a class is in Warning mode, all the resources in that class are in Warning mode.

Warning Mode only has an effect if Privileged Access Manager is in Full Enforcement mode.

### **NOTE**

Full Enforcement mode is the only mode Privileged Access Manager for UNIX supports. Privileged Access Manager for Windows also supports Audit Only mode.

You can use Warning mode when you introduce or modify an access policy. If you do this, you can examine the audit log to preview the results of your intended policy before you put that policy into effect. You can display the audit log by using the `seaudit` command.

If a class has the property *warning*, you can put the class into Warning mode. If a resource group or class is in Warning mode when an access rule is violated, Privileged Access Manager follows these steps:

- Allows the access
- Writes an entry in the audit log that references the resource (not the resource group or class)

The Warning mode settings on a resource and on a class are independent: if you put a resource into Warning mode, it remains in Warning mode, even if it belongs to a class and you remove Warning mode from that class.

#### NOTE

You can only put resources or classes into Warning mode if they have the property *warning*; not all resources or classes have this property.

### **Put a Resource into Warning Mode**

You put a resource into Warning mode to monitor the effects of access rules, without needing to enforce these rules.

To put a resource into Warning mode:

1. In Privileged Access Manager Endpoint Management, edit the resource that you want to put into Warning mode.  
The appropriate Modify page appears.
2. Click the Audit tab.  
The Audit Modes page for the resource appears.
3. Select Warning Mode, and click Save.  
The resource that you modified is now in Warning mode.

#### NOTE

In Warning mode, Privileged Access Manager always writes warning records to the audit log when access is permitted but access rules are violated: you do not need to set the audit property on the resource for this to happen.

**Example:** Put a file into Warning Mode:

The following selang example puts the file c:\myfile into Warning mode:

```
chres FILE c:\myfile warning
```

**Example:** Clear Warning Mode from a file:

The following selang example takes the file c:\myfile out of Warning mode:

```
chres FILE c:\myfile warning-
```

Warning mode is now not active for the myfile, so Privileged Access Manager enforces the access rules for myfile.

**Example:** Put a terminal into Warning Mode:

The following selang example puts the terminal myterminal into warning mode:

```
chres terminal myterminal warning
```

Privileged Access Manager permits access by any authorized user from the terminal myterminal. However, the product logs an audit record for any user that typically would be denied access from that terminal.

### **Put a Class into Warning Mode**

Rather than putting individual records into Warning mode, you can put all records in a class into Warning mode. You might use Warning mode to monitor the effects of access rules, without needing to enforce these rules.

#### **To put a class into Warning mode**

1. In Privileged Access Manager Endpoint Management, do as follows:
  - a. Click Configuration.
  - b. Click Class Activation.
 The Class Activation page appears.

2. Select the check box in the Warning column for the class you want to put into Warning mode.
3. Click Save.  
A confirmation message appears, letting you know that Privileged Access Manager options have been successfully updated.

### **Find Out Which Resources Are in Warning Mode**

Use Warning mode as a temporary measure when implementing Privileged Access Manager. Once you are comfortable that users have the required access to the resources they require, turn off Warning mode and Privileged Access Manager starts enforcing the associated rules.

To find out which resources are in Warning mode, create a report that shows all resources with Warning mode.

To create a report, enter the following command:

```
sereport -f pathname.html -r 6
```

Privileged Access Manager creates the report.

#### **NOTE**

For more information about the sereport utility, see the *Reference Guide*.

### **Find Out Which Classes Are in Warning Mode**

You should use Warning mode as a temporary measure when implementing Privileged Access Manager. Once you are comfortable that users have the required access to the resources they require, turn off Warning mode and Privileged Access Manager starts enforcing the associated rules.

To find out which classes are in Warning mode, you can get Privileged Access Manager to display this data.

To display this data, enter the following selang command:

```
setoptions cwarnlist
```

Privileged Access Manager displays a table showing the classes that are in Warning mode.

#### **NOTE**

For more information about setoptions, see the *selang Reference Guide*.

### **How to Perform System Maintenance**

At certain times you might need to perform system maintenance to upgrade the system, install a new application, and so on. During system maintenance set Privileged Access Manager rules in Warning mode. Once you are comfortable that the maintenance did not affect user access to resources that they require, turn off Warning mode and Privileged Access Manager startd enforcing the associated rules.

To use Warning mode when you perform system maintenance, do the following:

1. Set the appropriate classes to Warning mode before you start the maintenance, using the following selang rule:

```
setoptions class(NAME) flags(W)
```

2. Perform the maintenance.
3. Run the sereitrust utility after you perform the maintenance.  
The sereitrust utility generates the selang commands required to retrust programs and secure files defined in the database.
4. Run the selang command to retrust the programs defined in the database.
5. Remove the Warning mode from the classes to enable policy enforcement, using the following selang rule:

```
setoptions class(NAME) flags-(W)
```

6. Review Privileged Access Manager audit log files.

The audit log contains warnings for the resources that were affected by the maintenance.

#### NOTE

For more information about the `seretrust` utility, see the *Reference Guide*.

## Monitor Access Control Activity

The Privileged Access Manager trace is a real-time log that can show every action taken by the product. Trace records are accumulated in `ACInstallDir\log\seosd.trace` (where `ACInstallDir` is the directory where you installed Privileged Access Manager).

Or they are accumulated in whatever file you specify as the `trace_file` value in the registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSD\
```

Although you can filter the records from the trace file, the trace mechanism is designed for system monitoring and not for security auditing.

By default, Privileged Access Manager only generates trace messages during product initialization. Once Privileged Access Manager is initialized, it stops the trace mechanism and trace messages are not generated.

### Trace Record Filters

Privileged Access Manager generates two types of trace records:

- User trace records: Records actions completed by the user. Example: user1 accessed file `c:\tmp\tmp.exe`
- General trace records: Records actions completed by the system. Example: the Watchdog set a program to be nontrusted

Trace records are written to the `seos.trace` file, and can be filtered using the `trcfilter.ini` file.

If you set a user to be traceable, each time a trace record is written for that user, a matching audit record is written to the `seos.audit` file. The `audit.cfg` file filters the audit records.

#### NOTE

Audit records generated by trace events are not cached, and always go through the full enforcement flow.

The following `selang` command sets a user to be traceable:

```
editusr userName audit(trace)
```

To view trace or audit records, use the `seaudit` utility.

### Filter Trace Records

Using a trace filter file, you can specify that certain types of activity should not appear in the trace file. The trace filter file is specified with the `trace_filter` value in the registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSD
```

The default value is `ACInstallDir\log\trcfilter.ini` (where `ACInstallDir` is the directory where you installed Privileged Access Manager).

#### WARNING

Privileged Access Manager creates the trace filter file at installation with the single line: `*seosd.trace*`. Never delete this record.

Each line in the trace filter file represents an access or an activity that should *not* be traced. For example, to eliminate tracing the users' access to Microsoft Word, add the following line to the trace filter file:

```
*winword.exe*
```

## What Privileged Access Manager Server Control Audits

For security auditing, Privileged Access Manager keeps audit records for intercepted events according to the audit rules defined in the database and the enforcement mode it operates in. The records in the audit log accumulate according to these audit rules.

Full auditing provides audit records for all intercepted events of the following types:

- File access (FILE class)
- Program execution (PROGRAM class)
- Registry access (REGKEY and REGVAL classes)
- Impersonation control (SURROGATE class)
- Network control (CONNECT, TCP, HOST, GHOST, HOSTNET, and HOSTNP classes)
- Log in (TERMINAL class)

### NOTE

Intercepted login events are not cached; they always follow the auditing process for interception events.

- Service protection (WINSERVICE class)
- Password verification failure (PASSWORD class)
- Process termination (PROCESS class)

The decision whether to log an event depends on the Privileged Access Manager interception mode.

## Login Interception Limitations

Login interception on Windows is supported only by Privileged Access Manager sub-authentication method.

You cannot set login interception through the kernel. As a result, consider the following:

- Since the sub-authentication component works on the Domain Controller (DC) level, and it is up to the OS to decide which DC authenticates the user's login events (and triggers the Privileged Access Manager sub-authentication module), in a Windows domain environment, the product needs to be installed on every DC. When working in a Windows domain environment, Privileged Access Manager login policy (TERMINAL rules) need to be located on the DCs and not necessarily on the target server. For example, to protect or audit login events that are made by domain users on a file server, which is part of the Windows domain but is not a DC, define the Privileged Access Manager login policy on the DC and not on the target file server. This is because when a domain user accesses the shared file directory, a login authorization occurs on the DC, not the file server.
- When there is more than one DC, Privileged Access Manager login authorization could be processed on any one of the DCs. As a result, we recommend that you synchronize Privileged Access Manager login policy between all DCs. You can implement this synchronization through one of these methods:
  - The Policy Model mechanism, where all DCs are subscribers to a PMDB
  - Add all DCs into a host group and deploying a common policy using advanced policy management
- Some user properties, which correspond to login events, are updated at runtime during event authorization. These properties might be out-of-sync because the login authorization happens only on one of the DCs. These properties are *Gracelogins*, *Last accessed*, and *Last access time*. However, it is possible that the property *Last access time* value of the user is different between DCs because Privileged Access Manager sub-authentication was triggered on one of the DCs, not on all of them.
- To enforce local users' (that is, not domain users') login events, install Privileged Access Manager on the local computer that the local user needs access to. This is because the local computer is used as the domain computer (the domain is the local computer).
- Remote Desktop Protocol (RDP)/Terminal Services login events are enforced on the target server as it was in previous Privileged Access Manager versions. However, for RDP login events, Privileged Access Manager login policy should be defined on the target server.

### **What Privileged Access Manager Audits in Full Enforcement Mode**

In Full Enforcement mode (regular operation), Privileged Access Manager logs events as follows:

- If Warning mode is turned *off* for the intercepted resource, Privileged Access Manager enforces rules and logs the events based on the *audit* property of the resource or user.

| Audit Property | Events Logged    |
|----------------|------------------|
| ALL            | <i>All</i>       |
| SUCCESS        | Access permitted |
| FAIL           | Access denied    |

- If Warning mode is turned *on* for the intercepted resource, a record is written to the audit log if an access request violates an access rule (if the rules were enforced, the request would have failed). The audit record mentions that the violation was permitted because Warning mode is in effect.  
Rules are not enforced in this mode.

### **What Privileged Access Manager Audits in Audit Only Mode**

In Audit Only mode, Privileged Access Manager does not process requests for authorization or enforce rules. All intercepted login events for the accessor and all intercepted events for resources that are protected by Privileged Access Manager are logged, regardless of whether access failed or succeeded.

### **How to Change What Privileged Access Manager Writes to the Audit Log**

You can change what Privileged Access Manager writes to the audit log in two ways:

- Use the AUDIT property of the resources or accessors to define the audit events that Privileged Access Manager writes to the audit log.

#### **NOTE**

You can use the AUDIT property for a GROUP or XGROUP to set the audit property for all members of the group. However, you cannot use the AUDIT property to set the audit mode for group members if the audit mode of a user is defined in a USER record, XUSER record, or profile group.

- Use the audit configuration file audit.cfg to filter the events Privileged Access Manager sends to the audit log. You cannot use the audit.cfg file to add events to the audit log.

To reduce the number of audit records, you can also control consecutive audit events written to the log file. This customization is based on a time interval between consecutive matching audit events. That is, an access attempt to a resource with the same process ID, thread ID, rule ID, user ID, and access mask. The time interval, in seconds, can be set by setting the value of the AuditRefreshPeriod registry entry. By default, the AuditRefreshPeriod is set to zero (0), which means that all events are written to the log file.

### **Setting Audit Rules**

For security auditing, Privileged Access Manager keeps audit records for events of access denial or access grants according to the audit rules defined in the database.

Every accessor and resource has an AUDIT property that can be set to one or more of the following values:

- **FAIL**  
Logs access failures by the accessor to the resource.
- **SUCCESS**  
Logs successful accesses by the accessor to the resource.
- **LOGINFAIL**



Logs every logon failure by the accessor. (This value does not apply to resources.)

**NOTE**

Two types of login events are available: Password Attempt Event(A LOGIN) and Login Event(P/D/W LOGIN). For more information, see the *Reference Guide*.

**WARNING**

The Password Attempt Event is valid on UNIX only.

- **LOGINSUCCESS**

Logs every successful logon by the accessor. (This value does not apply to resources.)

- **ALL**

Logs the same information as FAIL, SUCCESS, LOGINFAIL, and LOGINSUCCESS for accessors or FAIL and SUCCESS for resources.

- **NONE**

Logs nothing concerning the accessor or resource.

Whenever you create or update an accessor or resource record in the database, you can specify the AUDIT property. You can also specify whether email notification of logged events should be sent and to whom.

The records in the audit log accumulate according to these audit rules. The decision whether to log an event is based on the following circumstances:

- If the resource or accessor has AUDIT(ALL), all login events for the accessor and all events concerning resources that are protected by Privileged Access Manager are logged. This logging occurs regardless of whether access failed or succeeded.
- If access to a resource protected by Privileged Access Manager is successful and the accessor or resource has AUDIT(SUCCESS), the event is logged.
- If access to a resource protected by Privileged Access Manager fails and the accessor or resource has AUDIT(FAIL), the event is logged.

In addition, if you set a user to be traceable, each time a trace record is written for that user, a corresponding audit record is written to the audit log.

### **Defining the Audit Events That Privileged Access Manager Writes to the Audit Log**

Privileged Access Manager writes access success and failures to the audit log. You define which access events Privileged Access Manager writes to the audit log, by changing the value of the AUDIT property for the resource or accessor that you want to audit. You can also use this method to specify that Privileged Access Manager logs every trace event to the audit log.

You use the AUDIT property to specify the audit events that Privileged Access Manager writes to the audit log. Use selang or Privileged Access Manager Endpoint Management to set the AUDIT property for resources and accessors as follows:

| Value of AUDIT | What Privileged Access Manager Logs                               | Applicable Objects  |
|----------------|-------------------------------------------------------------------|---------------------|
| FAIL           | Access failures                                                   | Users and resources |
| SUCCESS        | Access successes                                                  | Users and resources |
| LOGINFAIL      | Login failures                                                    | Users               |
| LOGINSUCCESS   | Login successes                                                   | Users               |
| ALL            | Equivalent to FAIL, SUCCESS, LOGINFAIL, LOGINSUCCESS, INTERACTIVE | Users and resources |
| TRACE          | Equivalent to ALL plus all system events                          | Users               |
| INTERACTIVE    | User sessions on UNIX computers                                   | Users               |

|      |            |                     |
|------|------------|---------------------|
| NONE | No logging | Users and resources |
|------|------------|---------------------|

**NOTE**

If the audit property of a user is not set, the AUDIT value of a group or profile group can affect the audit mode Privileged Access Manager uses for the user.

**How Privileged Access Manager Determines the Audit Mode for a User**

The audit mode for a user specifies which audit events Privileged Access Manager sends to the audit log for that user. The following process describes how Privileged Access Manager determines the audit mode for a user:

1. Privileged Access Manager checks if the record of the user in the USER or XUSER class has a value for the AUDIT property.  
If the record of the user has a value for the AUDIT property, Privileged Access Manager uses that value as the audit mode for the user.
2. Privileged Access Manager checks if the user is assigned to a profile group. If the user is assigned to a profile group, Privileged Access Manager checks if the record of the profile group in the GROUP class has a value for the AUDIT property.  
If the user is assigned to a profile group and the record of the profile group has a value for the AUDIT property, Privileged Access Manager uses that value as the audit mode for the user.
3. Privileged Access Manager checks if the user is a member of a group. If the user is a group member, Privileged Access Manager checks if the record of the group in the GROUP or XGROUP class has a value for the AUDIT property.  
If the user is group member and the record of the group has a value for the AUDIT property, Privileged Access Manager uses that value as the audit mode for the user. If the user is not a member of a group, or if the record of the group does not have a value for the AUDIT property, Privileged Access Manager assigns the systemwide audit mode to the user.

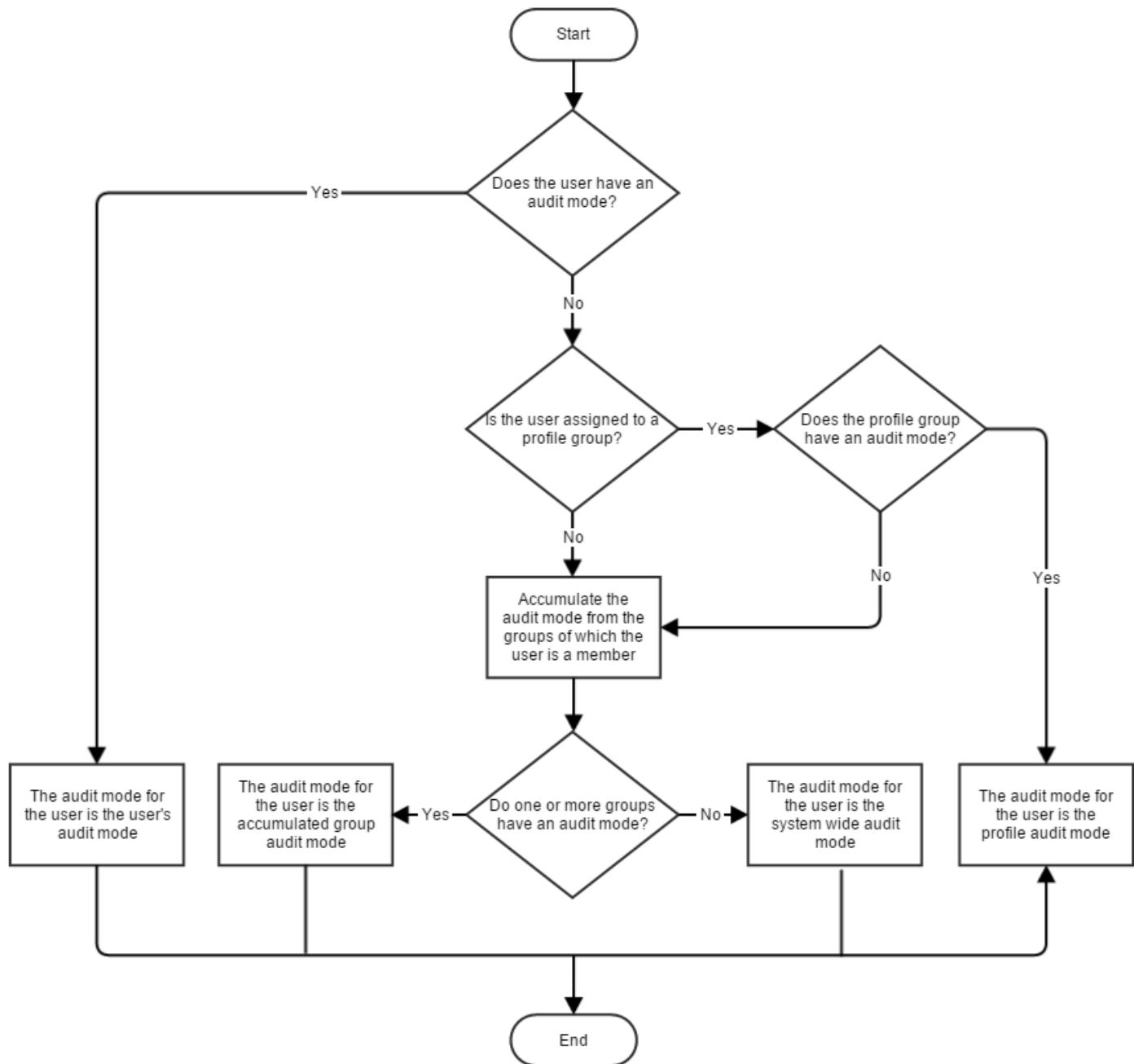
**NOTE**

The audit mode of the user accumulates if a user is a member of more than one group and the groups have different audit modes. The audit mode for the user is the sum of all the audit modes for the groups of which they are members.

**NOTE**

If Privileged Access Manager uses the value of a group's AUDIT property to determine the audit mode for a user, and you change the group's audit mode while the user is logged in, the audit mode for the logged-in user also changes. The user does not have to log off for the change in group audit mode to take effect.

The following diagram shows how Privileged Access Manager determines the audit mode for a user:

**Figure 45: Determine\_the\_Audit\_Mode\_for-a\_user****Example: Audit by Groups**

User Jan is a member of Group A and Group B. Group A has an audit mode of FAIL and Group B has an audit mode of SUCCESS. Because Jan is a member of both groups, Jan has the accumulated audit mode of FAIL and SUCCESS.

**Changing the Value of AUDIT Property for GROUP Records**

If you have a GROUP record that has two functions:

- A profile that defines an audit policy for one set of users
- A container for a second set of users

From r12.0 SP1 CR1 onwards, the GROUP record also defines the audit policy for the second set of users. To avoid problems that this behavior change may cause, create a separate GROUP for the second set of users.

### **Setting Audit Policies in Windows**

In addition to setting access rules for accessors and resources, you can specify Windows events that you want to write to the audit log. You can specify such audit policies for the entire organization, on a group basis, on a profile group basis, or on a user-by-user basis.

#### **Example: Set an Audit Policy for All Members of a Profile Group**

The following example sets an audit policy for all users that are part of a profile group:

1. Create a new profile group with the audit mode you require. For example:  

```
newgrp profileGroup audit(failure) owner(nobody)
```
2. Create a new user and attach it to the profile group you created. For example:  

```
newusr user1 profile(profileGroup) owner(nobody)
```
3. Remove the audit setting of the user. For example:  

```
chusr user1 audit-
```

You can now check whether this setting is effective:

1. Log on as the new user:  

```
runas /user:user1 cmd.exe
```
2. From the command prompt window of user1, enter the following command:  

```
secons -whoami
```

This command displays the information that is used for authorization and is held in the ACEE for user1.

```
ACEE audit mode is: Failure; Originated from Profile group definition
```

This message confirms that the audit policy is derived from the profile group the user is attached to.

#### **Example: Set a Audit Policy for Group Members**

In this example, a fictional company that is named Forward Inc wants to use Privileged Access Manager to protect all files in the /production directory. The /production directory has full access permissions in the native environment.

Forward Inc wants to deny and audit any attempts to access the /production directory. However, Forward Inc permits read access to the /production directory for developers. This access is not audited. An attempt by a developer to write to the /production directory is denied and audited.

Developers can request full access to the /production directory. Forward Inc audits any activity that a user with full access performs in the /production directory.

The following process describes the steps Forward Inc takes to implement the previous scenario:

1. Create a group named Developers in the native environment. Join all the developers to this group.
2. Create a group named Dev\_Access\_All in the native environment. Do not join any users to this group.
3. Define a generic access rule for the /production directory, as follows:

```
authorize FILE /production/* access(none) uid(*)
```

This rule sets the default access as none.

4. Define a generic audit rule for the /production directory, as follows:

```
editres FILE /production/* audit(failure)
```

This rule audits any failed attempt to access the /production directory.

5. Define an access rule for the Developers group, as follows:

```
authorize FILE /production/* access(read) xgid(Developers)
```

This rule permits members of the Developers group to have read access to the /production directory.

**NOTE**

The rule that you set in Step 4 ensures that Privileged Access Manager audits any failed access attempt by any user, including members of the Development group.

6. Define an access rule for the Dev\_Access\_All group, as follows:

```
authorize FILE /production/* access(all) xgid(Dev_Access_All)
```

This rule permits members of the Dev\_Access\_All group to have full access to the /production directory.

7. Define an audit rule for the Dev\_Access\_All group, as follows:

```
chxgrp Dev_Access_All audit(all)
```

This rule audits every action a member of the Dev\_Access\_All group performs.

8. When a member of the Developers group needs full access to the /production directory, add the user to the Dev\_Access\_All group in the native environment.

The user has full access to the /production directory, and Privileged Access Manager audits every action the user performs.

**NOTE**

The user must start a new logon session for the change in group membership to take effect.

9. When the user has completed their task in the /production directory, remove the user from the Dev\_Access\_All group in the native environment.

The user now has read access to the /production directory. Privileged Access Manager denies and audits any other access attempt on the /production directory by the user.

**NOTE**

The user must start a new log in session for the change in group membership to take effect.

## The Auditing Process

To configure Privileged Access Manager for your auditing requirements, you must first understand how auditing works. Auditing lets you keep track of access requests (events) that Privileged Access Manager intercepted. You can use this data to meet with compliance requirements, to analyze and refine your access rules for your security requirements, or to monitor access requests.

The process Privileged Access Manager follows to record audit events in the log depends on the type of event it intercepts:

- Interception events

**NOTE**

Intercepted login events (TERMINAL class), and audit records generated by user traces, are not cached; they always follow the auditing process for interception. events.

- [Audit events](#)

**NOTE**

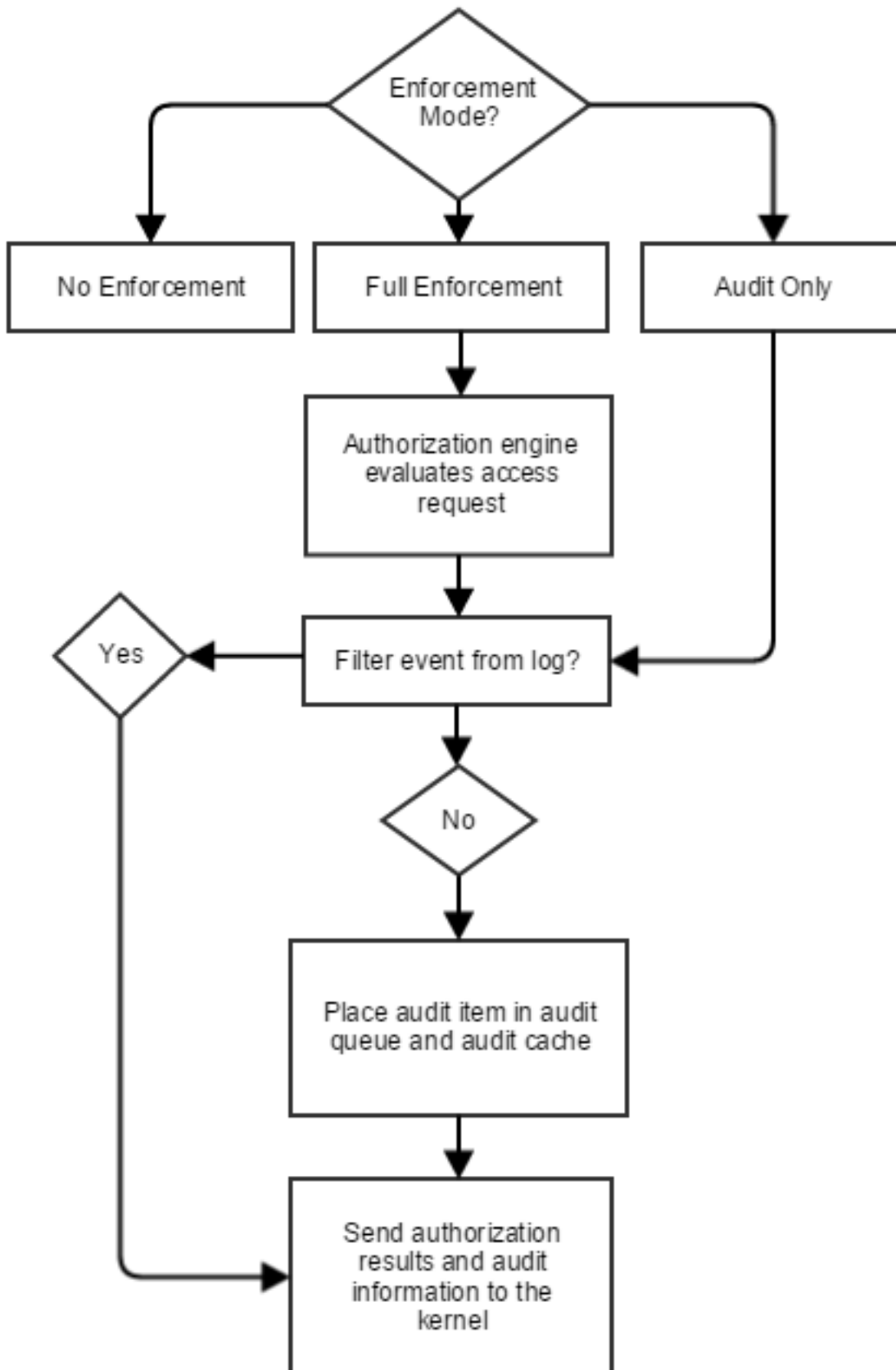
Privileged Access Manager intercepts an event only if the appropriate class is active, and the database contains a rule anticipating this event.

## How Auditing Works for Interception Events

An *interception event* is an event that Privileged Access Manager encounters for the first time and for which no authorization information or audit information exists in the kernel cache.

To log audit records, Privileged Access Manager performs the following actions and causes these effects for an interception event:

Figure 46: Audit Record Interception Events



- In No Enforcement mode, events are not intercepted or audited.
- In Full Enforcement mode, Privileged Access Manager follows these steps:
  - a. The authorization engine places an audit item that is based on the authorization result in the audit queue and in the audit cache.  
Privileged Access Manager writes an audit item only if the audit property for the resource or accessor is set to audit the resulting event and the audit filter file is not set to filter this event.
  - b. The authorization engine returns an informative answer on the authorization result and the audit-related information to the kernel.
- In Audit Only mode, Privileged Access Manager does not process the request for authorization. Audit information is always written, regardless of the audit property of the resource and user.  
Privileged Access Manager writes an audit item only if the audit filter file is not set to filter this event. The authorization result in this mode is always *P* (permitted).

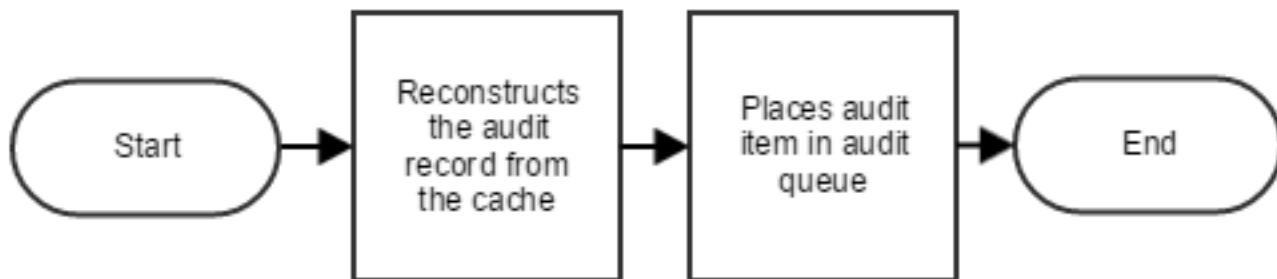
**NOTE**

Intercepted login events (TERMINAL class), and audit records that user traces generate are not cached. The authorization engine always writes audit records for these events.

**How Auditing Works for Audit Events**

The following diagram and steps demonstrate how auditing works for audit events:

**Figure 47: How Auditing Works for Audit Events**



Once the kernel notifies Privileged Access Manager about the cached interception event, Privileged Access Manager performs the following actions to log the audit event:

1. Reconstructs the audit data using the audit cache out of the information that the kernel sends.
2. Puts the audit item in the audit queue

**Kernel and Audit Caches**

The *kernel cache* contains data about previously intercepted events. The kernel identifies such cached intercepted events (audit events) and sends them to Privileged Access Manager for processing. Essentially, Privileged Access Manager uses the kernel cache to intercept events that follow the same pattern as a previously intercepted event.

The *audit cache* contains data that lets Privileged Access Manager reconstruct reoccurring audit records and send them to the audit queue without needing to follow the authorization process. This means that intercepted events, for which enough information already exists in the cache (audit events), are processed quickly and added to the audit queue. The authorization engine provides the data that is stored in the kernel and audit caches from the result of the initial event it intercepted (the interception event).

**Cache Reset**

Privileged Access Manager clears both the kernel and audit caches in the following cases:

- Database changes  
Privileged Access Manager clears the entire cache when database information changes. New or modified access rules make an existing cache potentially inaccurate.
- Time checkpoint reached  
Privileged Access Manager clears the entire cache when a time checkpoint affects an authorization result for any event. At the time that a DAYTIME restriction property or a HOLIDAY class record changes, the authorization result may change too and the cache becomes potentially inaccurate.
- PROGRAM resource change  
Privileged Access Manager clears the entire cache when the watchdog identifies that a PROGRAM resource has changed and become untrusted. An untrusted program affects the result of an authorization request regarding that program. This makes the cache potentially inaccurate.
- Audit cache filling  
Privileged Access Manager clears 10 percent of cache items (the least recently used items) when the audit cache fills up.

Once the cache is cleared, information from new interception events is needed to refill the cache and let Privileged Access Manager intercept an audit event.

## View Audit Event Logs

Privileged Access Manager sends audit events to the audit logs. You view the audit logs using the following Privileged Access Manager tools:

- Privileged Access Manager Endpoint Management
- The seaudit utility

You can configure Privileged Access Manager to send audit events to the Windows event log. The event log stores audit events from various applications in a single collection. You use the Windows Event Viewer to view audit events in the event log.

### Audit Events in the Windows Event Log

The Windows event log stores audit events from various sources in a single collection. If you configure Privileged Access Manager to route audit events to the event log, each time seosd writes an audit event to the Privileged Access Manager audit log, a corresponding event is sent to the event log.

The audit.cfg file filters audit events from both the audit log and the event log. If an audit event is not written to the audit log, it is not sent to the event log.

The Windows 2008 event log also routes audit events into containers that are called channels, depending on the volume, audience, and originating application of the audit events. The Privileged Access Manager channel is named CA-AccessControl-AuthorizationEngine/Audit.

If you have deployed Privileged Access Manager on a Windows 2008 server, you can choose to send audit events to:

- The event log
- The channel
- Both the event log and the channel
- Neither the event log or the channel

### Route Audit Events to the Windows Event Log

If you configure Privileged Access Manager to route audit events to the Windows event log, each time seosd writes an audit event to the Privileged Access Manager audit log, a corresponding event is sent to the event log. You can also configure Privileged Access Manager to send Policy Model audit events to the event log.



## To route events to the event log

1. Stop Privileged Access Manager using the following command:

```
secons -s
```

Privileged Access Manager stops.

2. Set the value of the SendAuditToNativeLog configuration setting in the logmgr section to 1.  
Audit events are sent to the Windows event log.
3. (Optional) Set the value of the SendAuditToNativeLog configuration setting in the Pmd section to 1.  
Audit events for policy models are sent to the Windows event log.
4. Restart Privileged Access Manager using the following command:

```
seosd -start
```

Privileged Access Manager restarts.

### Example: Route Audit Events to the Event Log

The following example routes audit events to the event log. You must be in the remote configuration environment (env config) to use this command:

```
er config ACROOT section(logmgr) token(SendAuditToNativeLog) value(1)
```

### Example: Route Policy Model Audit Events to the Event Log

The following example routes Policy Model audit events to the event log. You must be in the remote configuration environment (env config) to use this command:

```
er config ACROOT section(Pmd) token(SendAuditToNativeLog) value(1)
```

## Route Audit Events to the Windows Event Log Channel

### Valid for Windows Server 2008 only

If you configure Privileged Access Manager to route audit events to the Windows event log channel, each time seosd writes an audit event to the Privileged Access Manager audit log, a corresponding event is sent to the event log channel. The Privileged Access Manager event log channel is named CA-AccessControl-AuthorizationEngine/Audit.

You can also configure Privileged Access Manager to send Policy Model audit events to the event log channel. The Policy Model event log channel is named CA-AccessControl-Policy Models/Audit.

## To route events to the event log channel

1. Stop Privileged Access Manager using the following command:

```
secons -s
```

Privileged Access Manager stops.

2. Set the value of the SendAuditToNativeChannel token in the logmgr registry subkey to 1.  
Audit events are sent to the Windows event log channel.
3. (Optional) Set the value of the SendAuditToNativeChannel token in the Pmd registry subkey to 1.  
Policy Model audit events are sent to the Windows event log channel.
4. Restart Privileged Access Manager using the following command:

```
seosd -start
```

Privileged Access Manager restarts.

### Example: Route Audit Events to the Event Log Channel

The following example routes audit events to the event log channel. You must be in the remote configuration environment (env config) to use this command:

```
er config ACROOT section(logmgr) token(SendAuditToNativeChannel) value(1)
```

### Example: Route Policy Model Audit Events to the Event Log Channel

The following example routes Policy Model audit events to the event log channel. You must be in the remote configuration environment (env config) to use this command:

```
er config ACROOT section(Pmd) token(SendAuditToNativeChannel) value(1)
```

### The Audit Log (Windows)

The audit log is stored in a file. The value *audit\_log* in the following Windows registry subkey specifies the location of the audit log file:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\logmgr
```

The default value for this key is:

```
C:\Program Files\CA\PAMSC\log\seos.audit
```

By default, Privileged Access Manager automatically backs up the audit log when it reaches 1024 KB. You can change this size by changing the value *audit\_size* in the subkey:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\logmgr
```

You can also back up the audit log periodically (daily, weekly, or monthly). To do so, change the value *BackUp\_Date* in the Windows registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\logmgr
```

#### NOTE

For more information about these registry subkeys, see the *Reference Guide*.

### Using Audit Logs

Privileged Access Manager provides two built-in tools for viewing, filtering, and searching the audit logs:

- Privileged Access Manager Endpoint Management
- The seaudit utility

You can display every record in the audit log. You can also use filters to select particular records from the audit log.

The remainder of this topic describes how to view the records in the audit log when using audit filters in Privileged Access Manager Endpoint Management.

### Audit Record Filters

The audit.cfg file filters audit records on a host by defining records that should not be sent to the audit file. Each line in the file represents a rule for filtering out audit information. The records that match the criteria in the line do not appear in the audit file. This filter helps to limit the size of the seos.audit file by keeping only the records needed. You can edit the audit.cfg file to suit your enterprise requirements.

By default, the audit.cfg file is located in the *ACInstallDir/etc* directory (UNIX) or *ACInstallDir\data* directory (Windows). You can change the location of the audit.cfg file by editing the [logmgr] AuditFiltersFile token in the seos.ini file (UNIX), or the AuditFiltersFile entry in the logmgr registry key (Windows).

The Privileged Access Manager Engine, seosd, reads the audit.cfg file at startup. When a message is sent to the audit file, seosd checks if the message matches one of the rules in the audit.cfg file. If the message matches a rule, the message is not written to the audit file.

#### NOTE

For more information about the audit.cfg file, see the *Reference Guide*.

### Audit Display Filters

The number of records in the audit log can become enormous. To reduce the number of records that *display*, use filters to specify the types of records for display. You can filter events by various criteria, including time or event type.

#### NOTE

You can also filter the audit records Privileged Access Manager *writes* to the audit file using the audit configuration settings (audit.cfg file).

You can create a filter in Privileged Access Manager Endpoint Management simply by giving it a name and choosing at least one switch. You can then select more switches, and have the option of assigning one or more options. You can also filter records with the seaudit utility.

Privileged Access Manager Endpoint Management provides several predefined filters, and you can create your own filters.

#### **Filter Wizard, Choose Name and Switches Page**

The Choose Name and Switches page of the Filter Wizard lets you define the following parameters:

- The name of the audit display filter you want to create
- The switches that you want to apply to this filter

This window contains the following fields:

- **Filter Name**  
Defines the name of the audit display filter you want to create.
- **Audit Event Records**  
Specifies whether you want the filter to display all audit records or only those switches that are selected. If you select to list all records, the switches on this page do not apply.
- **List INET audit records of Host and Service**  
Specifies whether to list the INET audit records of the TCP requests received from the specified hosts for the specified services. Host and service are masks that identify which set of hosts and services are searched for.
- **Show LOGINs for user on terminal**  
Specifies to list the following information:
  - LOGIN records for the specified user on the specified terminal. Both *user* and *terminal* are masks that you define.
  - Records created by the authorization engine when an invalid password is entered multiple times.
- **List RESOURCES audit of class on resource for users**  
Specifies whether to list resource records. You can define the following later:
  - *Class*, a mask that identifies the class to which the accessed resource belongs.
  - *Resource*, a mask that identifies the names of the resources that were accessed.
  - *User*, a mask that identifies the name of the users who accessed the resources.
- **List updates to database**  
Lists database update audit records. You can define:

- *Cmd*, a mask identifying the selang commands to search for.
- *Class*, a mask identifying the classes to search for.
- *Object*, a mask identifying the records to search for.
- *User*, a mask identifying the users who executed the commands.
- **List startup/shutdown messages**  
Specifies whether to list the startup and shut down messages from the Privileged Access Manager services.
- **List WATCHDOG audit records**  
Specifies whether to list the Watchdog audit records.
- **Show only trace records**  
Specifies whether to only list records sent to the audit log by the tracing facility.

### ***Filter Wizard, Edit Options Page***

The Edit Options page of the Filter Wizard lets you define the options that you want to apply to audit display filter.

This window contains the following fields:

- **Listing's Starting Today**  
Specifies today as the start date. Records that are logged before today are not listed.
- **Listing's Starting Date**  
Specifies the start date. Records that are logged before the specified date are not listed.
- **Listing's Starting Time**  
Specifies the start time. Records that are logged before the specified time are not listed.
- **Listing's Ending Date**  
Specifies the end date. Records that are logged after the specified date are not listed.
- **Listing's Ending Time**  
Specifies the end time. Records that are logged after the specified time are not listed.
- **Show Internet address not host name**  
Specifies that Internet addresses be listed instead of host names in TCP/IP records.
- **Hide failures**  
Specifies that failures are not listed.
- **Hide any granted accesses**  
Specifies that successful (granted) accesses are not listed.
- **Hide logout records**  
Specifies that logout records are not listed.
- **Hide NOTIFY audit records**  
Specifies that NOTIFY audit records are not listed.
- **Hide passwords attempts and actions**  
Specifies that password attempt records are not listed.
- **Hide warning records**  
Specifies that warning records are not listed.
- **Show port numbers not names**  
Specifies that port numbers be listed instead of service names.
- **Show only records originated from *host***  
Specifies that only records originating from the specified host are listed. This option is applicable only when connected to a UNIX workstation.

### ***Predefined Filters***

Privileged Access Manager comes with the following predefined filters:

- **All records**  
Displays every record in the audit log. No filtering takes place.
- **Today's records**

Shows every record created today.

- **Last 2 days records**

Shows every record created yesterday and today.

- **Last 7 days records**

Shows every record created during the last seven days.

- **Connections to Privileged Access Manager services**

Shows records that indicate when users connect to Privileged Access Manager services such as Privileged Access Manager Endpoint Management or selang.

**NOTE**

When connecting to a UNIX workstation, the name for this filter becomes Login Records. The records represent user logins.

- **Administration activity**

Shows all records that update the Privileged Access Manager or operating system databases. Updates to the databases include adds, deletes, and changes to all types of records.

### **Create a User-Defined Filter**

You can build as many filters as you need. Create a custom filter when you want to view only a particular set of audit records.

#### **To create a user-defined filter**

1. In Privileged Access Manager Endpoint Management, click the Audit Events tab.  
The Audit Records Viewer's Filter Settings section shows the list of Saved Filters.
  2. In the Saved Filters section, click Create Filter.  
The Audit Filter Wizard appears.
  3. Complete the wizard pages.
    - **Choose Name and Switches**  
Specifies the [switches that you want](#) to use in your filter.
    - **Edit Switches**  
Specifies settings for the switches you selected. These settings are masks that you can define for the audit events you want to filter.
    - **Edit Options**  
Specifies the [options that you want](#) to set for audit filtering.
- Click **Finish**.  
The new audit filter that you defined is saved and loaded.

### **Audit Log Backup**

Privileged Access Manager lets you automatically backup the audit log file for archiving.

The name of the audit log backup file is set in the logmgr\audit\_back Privileged Access Manager registry entry.

You can use the following methods for backing up the audit log file:

- Size-triggered backups
- Date-triggered backups

The method and settings you choose for backing up your audit log file depend on:

- Whether you need backup copies of the log file
- How much auditing data is likely to be generated in your environment
- System performance issues (for example, larger audit log files increase processing time)

**NOTE**

By default, Privileged Access Manager protects audit log backup files if you configure settings to keep timestamped backups. This is the same default protection that the size-triggered audit backup file receives. To remove these files, set permissive rules in the database.

**Set the Size at which the Audit Log is Backed Up Automatically**

You can set a limit on the size of the audit log file. When the file reaches the defined size, Privileged Access Manager automatically creates a backup copy of the file and clears the log. This means that the file is automatically backed up regularly.

To set the size at which the audit log is backed up automatically, set the maximum size that you require, in KB, in the logmgr\audit\_size Privileged Access Manager registry entry.

**NOTE**

You can define the name of the backup file by setting the logmgr\audit\_back Privileged Access Manager registry entry.

**WARNING**

If the logmgr/BackUp\_Date Privileged Access Manager registry entry is set to yes (no is the default), each size-triggered backup copy of the audit log is suffixed with a timestamp. In all other cases, including when date-triggered backups are configured, each backup copy *overwrites* the previously written backup copy.

**Example: Set automatic backup of audit log file when it reaches 5 MB**

This example shows you how you set your audit log file to be backed up when it reaches 5 MB (5120 KB). To do this, set the logmgr\audit\_size Privileged Access Manager registry entry to **5120**.

When the audit log file reaches 5 MB, Privileged Access Manager creates a backup copy of the file, named seos.audit.bak by default, and clears the log.

**Example: Set automatic backup of audit log file when it reaches 1 MB with a custom name and a timestamp**

This example shows you how you set your audit log file to be backed up when it reaches 1 MB (1024 KB), using a custom name for the backup file and adding a timestamp to the name.

To do this, set the following Privileged Access Manager registry entries as shown:

- logmgr\audit\_size=1024
- logmgr\audit\_back=log\ac\_audit.old
- logmgr\BackUp\_Date=yes

When the audit log file reaches 1 MB, Privileged Access Manager creates a backup copy of the file, and clears the log. The name of the backup log file name is: ac\_audit.old.*timestamp*, where *timestamp* is the date and time in the format DD-Mon-YYYY.hhmmss. For example:

```
ac_audit.old.06-Feb-2007.144330
```

**Set the Time Interval at Which the Audit Log Is Backed up Automatically**

You can define a time interval (daily, weekly, or monthly) at which Privileged Access Manager automatically creates a backup copy of the audit log file and clears the log.

To set the time interval at which the audit log is backed up automatically, set the interval in the logmgr\BackUp\_Date Privileged Access Manager registry entry. The interval can be one of the following:

- **daily**  
Backs up the audit log file once a day.
- **weekly**

Backs up the audit log file once a week.

- **monthly**

Backs up the audit log file once a month.

**NOTE**

You can define the name of the backup file by setting the logmgr\audit\_back Privileged Access Manager registry entry.

**WARNING**

If the audit log reaches the size limit that is defined in the logmgr\audit\_size Privileged Access Manager registry entry before the backup interval is reached, the product creates a backup copy of the file without a timestamp.

Each such backup copy can potentially overwrite any previous copy.

**Example: Set a daily backup of the audit log file**

This example shows you how you set your audit log file to be backed up daily. To do this, set the logmgr\BackUp\_Date Privileged Access Manager registry to **daily**.

Once a day Privileged Access Manager creates a backup copy of the file, and clears the log. The backup log file name has the *.timestamp* suffix, where *timestamp* is the date and time in the format DD-Mon-YYYY.hhmmss. For example:

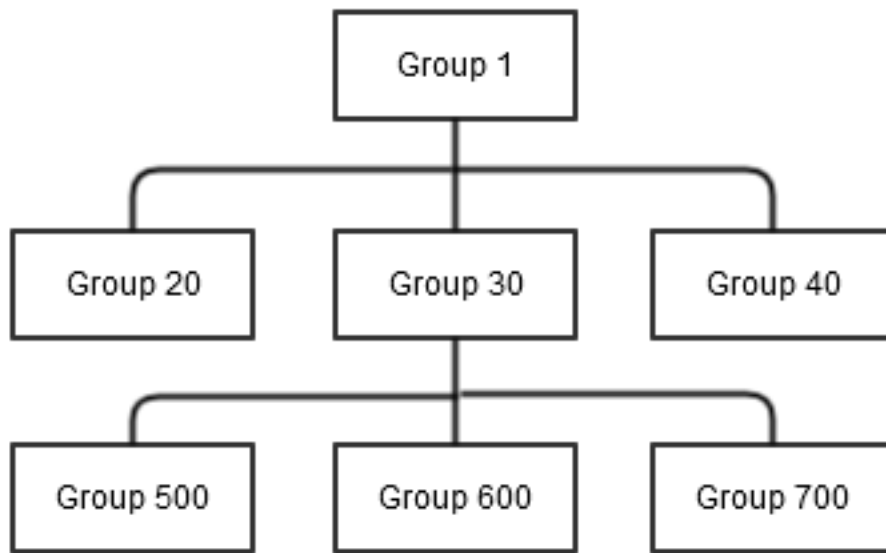
```
seos.audit.bak.06-Feb-2007.144330
```

## Group Authorization

It is necessary to understand the concept of parentage before discussing group authorization attributes.

### Parentage

The concept of subordinate and superior groups, also known as parentage, is important when discussing group administration privileges. One group can be the parent-superior-of one or more groups. A *child* or subordinate group can have only one parent. Assigning a parent to a group is optional. Consider the following diagram:

**Figure 48: parentage**

Group 1 is the parent of the three Groups 20, 30, and 40. Group 30 is also the parent of three groups-500, 600, and 700. Group 600 has only one parent-Group 30. Group 1 has no parent.

### **Group Authorization Attributes**

All records, including resource records and accessor records alike, have owners. Owning a record means having authorization to view, edit, and remove it.

A group can own its own records. However, within a group that owns records, only certain privileged users can manage the records. These special users have a group authorization attribute set in their own user records. The group authorization attributes are the following:

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

The join command-which only a properly authorized user can issue-sets these attributes. The join command serves the purpose of both putting a user into a group, and specifying the user's group authorization attribute (if any).

The privileged members of the group may or may not be authorized to manage the user records that define the members of the group, depending on who owns those records.

### ***GROUP-ADMIN Attribute***

Users with a group administration authorization attribute can create a certain set of records. In order to create a record, the group administrator has to specify the owner of the record.

The owner of the records must be the group in which the user has a group authorization attribute. If that group is the parent of other groups, the owner can also be from one of the sub groups. The whole set of records is called the group scope. The authorization examples provided illustrate the concept of group scope.



Users with the GROUP-ADMIN attribute have the following access authority for the records within their group scope:

| Access  | Description                                                     | Commands                            |
|---------|-----------------------------------------------------------------|-------------------------------------|
| Read    | Show the properties of the record.                              | showusr, showgrp, showres, showfile |
| Create  | Create new records in the database. You must specify the owner. | newusr, newgrp, newres, newfile     |
| Modify  | Change the properties of the record.                            | chusr, chgrp, chres, chfile         |
| Delete  | Remove records from the database.                               | rmusr, rmgrp, rmres, rmfile         |
| Connect | Join a user to a group or separate a user from a group.         | join, join-                         |

The GROUP-ADMIN attribute also has limits:

- GROUP-ADMIN users cannot make resources inaccessible to themselves, so:
  - GROUP-ADMIN users cannot assign a security level that is higher than their own security level.
  - GROUP-ADMIN users cannot assign a security category or security label that they do not have.
- GROUP-ADMIN users cannot delete the user superuser (the root account on UNIX or the Administrator account on Windows) from the database.
- Several limitations concern the global authorization attributes described in Global Authorization Attributes in this chapter:
  - A GROUP-ADMIN user cannot delete the only ADMIN user record in the database.
  - A GROUP-ADMIN user cannot remove the ADMIN attribute from the record of the last ADMIN user in the database.
  - GROUP-ADMIN users without the AUDITOR attribute cannot update the audit mode. Only a GROUP-ADMIN user with the AUDITOR attribute can update the audit mode.
  - GROUP-ADMIN users cannot set the global authorization attributes-ADMIN, AUDITOR, OPERATOR, PWMANAGER, and SERVER-for any user.

### **GROUP-AUDITOR Attribute**

A user with the GROUP-AUDITOR attribute can list the properties of any record within the group scope. The group auditor can also set the audit mode for any record within the group scope.

### **GROUP-OPERATOR Attribute**

A user with the GROUP-OPERATOR attribute can list the properties of any record within the group scope.

### **GROUP-PWMANAGER Attribute**

A user with the GROUP-PWMANAGER attribute can change the password of any user whose record is within the group scope.

## **Ownership**

Every record in the database—including both accessor records and resource records—has an owner. When you add a record to the database, you can either explicitly assign its owner by using the owner parameter or let Privileged Access Manager assign the user who defines the record as the owner of the record.

Accessors own a record if *any* of the following are true:

- They are defined as the owner of the record.
- They are members of a group that is defined as the owner of the record *and* they have joined the group with the GROUP-ADMIN property.
- They are owners of a resource group record that the resource is a member of.

If you remove a user or group that owns records from the database, the records no longer have an owner.

Users who own records have the following access authority for the records they own:

| Access  | Description                                             | Commands                            |
|---------|---------------------------------------------------------|-------------------------------------|
| Read    | Show the properties of the record.                      | showusr, showgrp, showres, showfile |
| Modify  | Change the properties of the record.                    | chusr, chgrp, chres, chfile         |
| Delete  | Remove the record from the database.                    | rmusr, rmgrp, rmres, rmfile         |
| Connect | Join a user to a group or separate a user from a group. | join, join-                         |

If you do not want a user or group to have ownership authority over a particular record, assign the owner *nobody* to the record and to any resource group record that the record is a member of.

The limits of the ownership privileges are as follows:

- The owner of the last ADMIN user in the database cannot delete that user record.
- Owners who do not have the AUDITOR attribute cannot update the audit mode. Only an owner with the AUDITOR attribute can update the audit mode.
- The owner of a superuser (the root account on UNIX or the Administrator account on Windows) cannot delete root from the database.
- Owners cannot set the global authorization attributes—ADMIN, AUDITOR, OPERATOR, and PWMANAGER—for the users they own.
- Owners cannot make resources inaccessible to themselves, so:
  - Owners cannot assign a security level that is higher than their own security level.
  - Owners cannot assign a security category or security label that they do not have.

## File Ownership

Privileged Access Manager allows the owner of a file to protect the file by defining a record in the FILE class. The owner of the file has full authority over the record of that file, so the owner can use the newfile, chfile, showfile, authorize, and authorize- commands with all parameters for the record that protect the file.

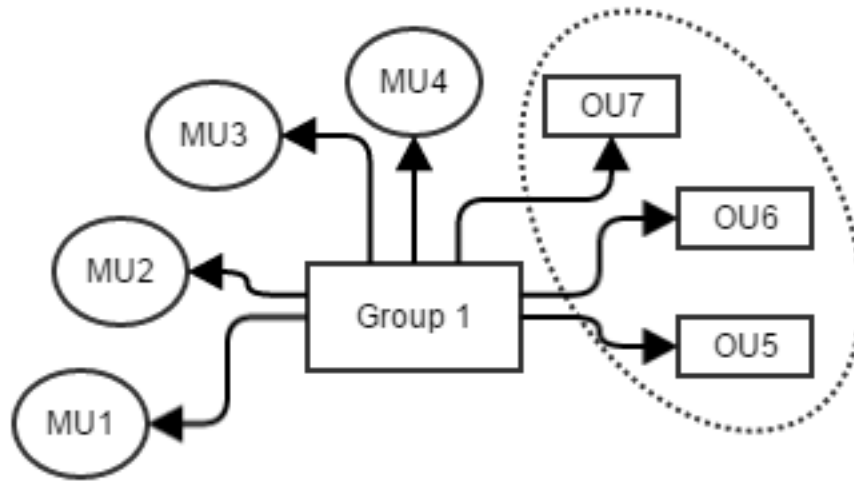
On UNIX, when a user creates a file, UNIX assigns the user as the owner of the file. Privileged Access Manager allows UNIX file owners to define FILE records, unless this feature is explicitly disabled. If you do not want file owners to define FILE records, make sure that the use\_unix\_file\_owner token in the [seos] section of the seos.ini file is set to no. (This is the default setting.)

## Authorization Examples

Following are diagrams that illustrate the concepts of group authorization attributes, parentage, ownership, membership, and group scope. These diagrams only contain users and groups, but the concept of ownership also applies to resource and file records.

### Single Group Authorization

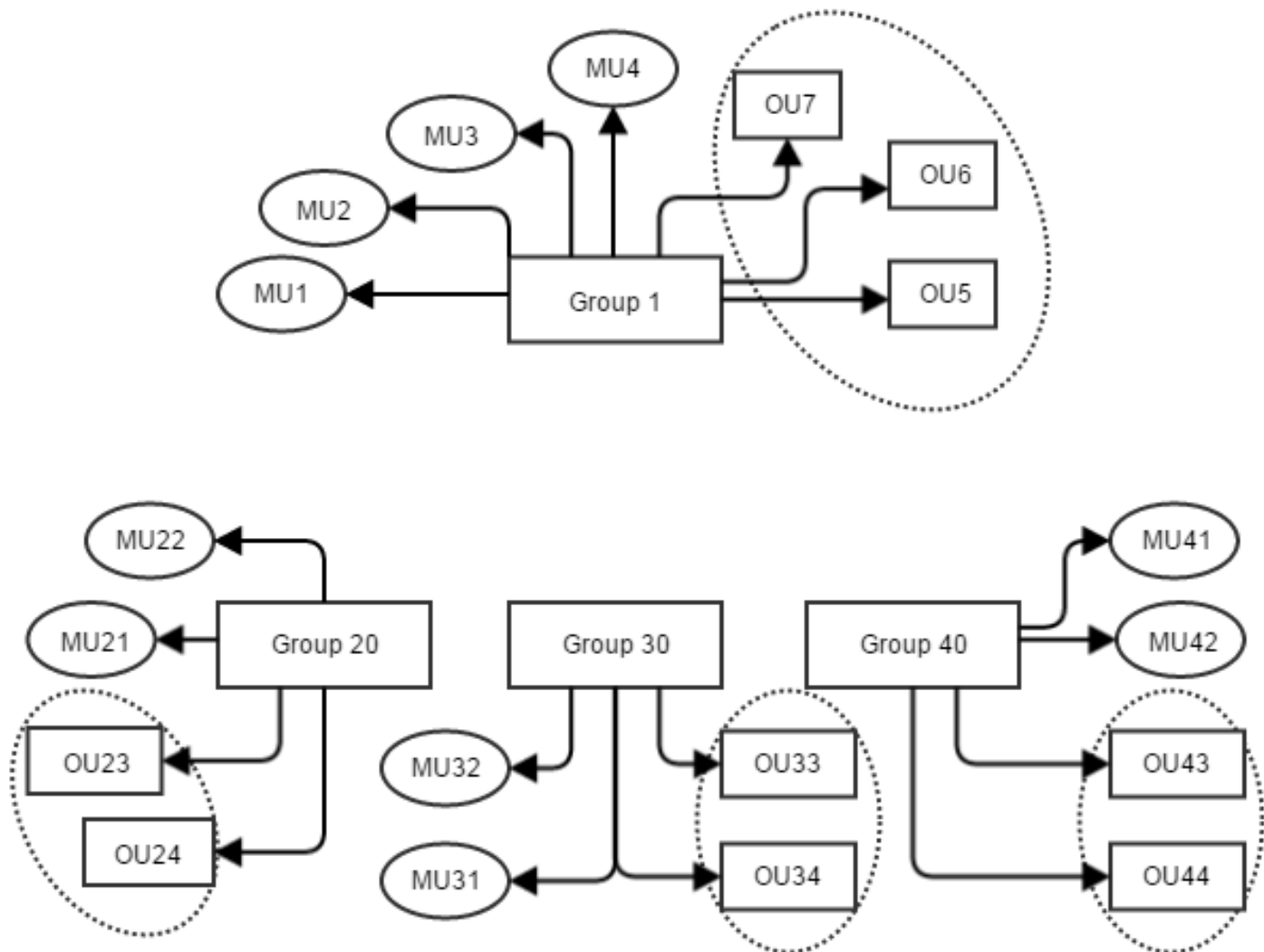
In the following diagram, four users are members of Group 1: MU1, MU2, MU3, and MU4. Group 1 also owns three users—OU5, OU6, and OU7. The member MU4 has the GROUP-ADMIN attribute.

**Figure 49: Single group authorization**

The ellipse indicates the group scope of the commands executed by user MU4. It includes all the users owned by Group 1-OU5, OU6, and OU7.

#### **Parent and Child Groups**

In the following diagram, four users are members of Group 1: MU1, MU2, MU3, and MU4. Group 1 also owns three users-OU5, OU6, and OU7. The member MU4 has the GROUP-ADMIN attribute set in its record.

**Figure 50: Parent and child groups**

Group 1 is also the parent of three groups—20, 30, and 40. Each of these subordinate groups has two users who are members of the group and two users who are owned by the group.

The four ellipses indicate the group scope of the commands executed by user MU4. It includes all the users owned by Group 1, as well as the users owned by the groups subordinate to Group 1. The users in the group scope of MU4 are OU5, OU6, OU7, OU23, OU24, OU33, OU34, OU43, and OU44.

If there were groups subordinate to Groups 20, 30, or 40 that owned users, groups, or resources, the records owned by these groups would also be in the group scope of commands executed by user MU4.

## **Windows Environment**

### **Valid in the native Windows environment**

When Privileged Access Manager is running, if you use `selang` to change a resource in the native Windows environment, the Privileged Access Manager Agent changes the resource in the appropriate Windows repository. You do not need any additional Windows permissions to change the resource. This means that when users in Privileged Access Manager with

global or group authorization attributes perform `selang` commands in the native Windows environment, they have the same privileges and limits for Windows as they do for Privileged Access Manager.

When Privileged Access Manager is not running, if you use `selang` to change a resource in the native Windows environment, you must follow these rules:

- You must include the `l` option in the `selang` command
  - You must have the ADMIN attribute or sub administration privileges
  - You must have sufficient Windows permissions to change the resource
- This restriction occurs because a `selang` process, not the Privileged Access Manager Agent, changes the resource in the Windows repository.

For example, user Emma wants to use the `chfile` `selang` command in the native Windows environment to change the owner of the file `C:\tmp.txt`. If Privileged Access Manager is running, Emma requires sufficient Privileged Access Manager permissions to change the file owner, but does not require additional Windows permissions. If Privileged Access Manager is not running, Emma requires both Privileged Access Manager and Windows permissions to change the file owner.

## **UNIX Environment**

For managing users and groups in UNIX, users in Privileged Access Manager with global or group authorization attributes have the same privileges and limits for UNIX as they do for Privileged Access Manager.

If you use `selang` while the `seosd` daemon is *not* running (for example, at installation time), you must follow these rules:

- You must include the `-l` option in the `selang` command.
- The user of `selang` must be root. (This exclusive root privilege complies with regular UNIX restrictions.)

## **Manage Sub Administrators**

Security administrators (users with the ADMIN attribute) can grant specific administrative privileges to regular users. These regular users are then called sub administrators. Sub-administrators have privileges to manage only specified Privileged Access Manager classes or objects. For example, a sub administrator can be authorized to manage only user and group objects. You can set a higher level of sub administration by authorizing the sub admin user the administrative privileges for specific objects in a class.

Sub administrators of users, groups and resources can use `selang` to perform administrative tasks related to these resources.

## **How to Grant Specific Administrative Privileges to Regular Users**

Because administrator users with the ADMIN attribute can execute almost all actions in Privileged Access Manager, you may want to delegate specific administrative tasks to sub administrators. To do this, grant those users with privileges to classes in the Privileged Access Manager database that control the specific administrative tasks the user needs to perform as follows:

1. Identify one or more classes that control the tasks you want to delegate.  
For example, Privileged Access Manager uses the USER and GROUP classes to create accessor resources. If you want to delegate accessor management, you need to use the USER and GROUP records of the ADMIN class.
2. Authorize one or more sub administrator to the applicable resource of the ADMIN class.  
For example, to let a sub administrator view and modify user records, grant the user with *read* and *modify* access to the USER record of the ADMIN class.

## **The ADMIN Class**

Sub administrator users listed in the access control list (ACL) of records in the class ADMIN have privileges similar to users with the ADMIN attribute. However, the privileges of users in the ACL for records in the class ADMIN are limited

to the particular class represented by the record. For example, the SURROGATE record in the ADMIN class determines which users can administer records of the SURROGATE class.

#### NOTE

For more information about Privileged Access Manager classes, see the *Reference Guide*.

A user in the ACL for a particular record in class ADMIN can execute the following commands:

| Access   | Description                                                                                                                                                                                                                             | Commands                                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Read     | Show the properties of the record in the class.                                                                                                                                                                                         | showusr, showgrp, showres, showfile, find |
| Create   | Create new database records in the class.                                                                                                                                                                                               | newusr, newgrp, newres, newfile           |
| Modify   | Change properties in the class.                                                                                                                                                                                                         | chusr, chgrp, chres, chfile               |
| Delete   | Remove existing class records from the database.                                                                                                                                                                                        | rmusr, rmgrp, rmres, rmfile               |
| Connect  | Add users to and remove users from groups. This access is valid only in the ACL of the GROUP record.                                                                                                                                    | join, join-                               |
| Password | Control the password of all users within the database, and their password attributes. This access grants the same authority as the access permitted a user with the PWMANAGER attribute. This is valid only in the ACL for record USER. | chusr                                     |

Users with ADMIN class privileges have the following limitations:

- Users defined in the ACL of the USER record in class ADMIN cannot delete the last ADMIN user in the database.
- ADMIN class users cannot set the global authorization attributes-ADMIN, AUDITOR, OPERATOR, and PWMANAGER- for the users they own.
- ADMIN class users cannot necessarily update the audit mode. Only an ADMIN class user with the AUDITOR attribute can update the audit mode.
- ADMIN class users cannot delete superuser (the root account on UNIX or the Administrator account on Windows), but they can set root to be NOADMIN.
- ADMIN class users cannot make resources inaccessible to themselves, so:
  - ADMIN class users cannot assign a security level to a resource that is higher than their own security level.
  - ADMIN class users cannot assign a security category or security label that they do not have.

These limitations are part of the B1 security level certification.

## Environmental Considerations

One of the factors governing whether you can update information in your database is the position you occupy in the environment.

### Remote Administration Restrictions

You can access a remote station over a network and can update the database on the remote station. To update the database on the remote station, both you and your terminal need permission.

- You must be explicitly defined as a user in the database of the remote station. For whatever commands you want to execute, set the appropriate attribute in your user record in the database of the remote station.
- Explicitly mention the needs of your local terminal in a rule granting it WRITE permission for accessing the remote station. Otherwise, you cannot perform Privileged Access Manager administration there.  
With WRITE permission through a default access field (`_default`), or through the UACC class, you can enter the `selang` command shell at the remote station. However, you *cannot* execute any `selang` commands or otherwise access to the remote database. With READ permission, you can log in to the remote station but you cannot perform Privileged Access Manager administration there.

Here is an example of this distinction between WRITE and READ permission:

- To specify a new terminal with READ as default access, where administrators can log in from the terminal but cannot manipulate the database from it, issue the following command:

```
newres TERMINAL tty13 defacc(read)
```

- To grant user ADMIN1 permission to manipulate the database from the new terminal (that is, grant WRITE permission and READ permission), issue the following command:

```
authorize TERMINAL tty13 uid(ADMIN1) access(r,w)
```

## UNIX Environment

For managing users and groups in UNIX, users in Privileged Access Manager with global or group authorization attributes have the same privileges and limits for UNIX as they do for Privileged Access Manager.

If you use `selang` while the `seosd` daemon is *not* running (for example, at installation time), follow these rules:

- Include the `-l` option in the `selang` command.
- The user of `selang` must be root. (This exclusive root privilege complies with regular UNIX restrictions.)

## Windows Environment

### Valid in the native Windows environment

When Privileged Access Manager is running, the Privileged Access Manager Agent changes the resource in the appropriate Windows repository if you use `selang` to change a resource in the native Windows environment. You do not need any additional Windows permissions to change the resource. This means that when users in Privileged Access Manager with global or group authorization attributes perform `selang` commands in the native Windows environment, they have the same privileges and limits for Windows as they do for Privileged Access Manager.

When Privileged Access Manager is not running, if you use `selang` to change a resource in the native Windows environment, follow these rules:

- Include the `l` option in the `selang` command
- You must have the ADMIN attribute or sub administration privileges
- You must have sufficient Windows permissions to change the resource  
This restriction occurs because a `selang` process, not the Privileged Access Manager Agent, changes the resource in the Windows repository.

For example, user Emma wants to use the `chfile` `selang` command in the native Windows environment to change the owner of the file `C:\tmp.txt`. If Privileged Access Manager is running, Emma requires sufficient Privileged Access Manager permissions to change the file owner, but does not require more Windows permissions. If Privileged Access Manager is not running, Emma requires both Privileged Access Manager and Windows permissions to change the file owner.

## Default Permissions to Access the Database

Privileged Access Manager protects the internal database, `seosdb`, with internal file rules when it is running. Internal file rules are not visible in `selang` and cannot be deleted. You can write FILE rules to override the internal file rules. If you delete these FILE rules, Privileged Access Manager reverts to the internal file rules.

The following internal file rules protect the database when Privileged Access Manager is running:

- Privileged Access Manager internal processes have full access to the database.
- The NT AUTHORITY\System user has read access to the database.
- All other accessors have no access to the database.

#### NOTE

The default access rights for all other accessors were changed in r12.5 SP3. In previous releases, all other accessors had read access by default to the database files.

By default, Privileged Access Manager services run automatically after you install Privileged Access Manager or reboot the endpoint. Consequently, the only user who can access the database out of the box is NT AUTHORITY\System. The Privileged Access Manager administrators that you define during installation can also use a utility such as `selang` to update the database.

## Native Permissions to Access the Database

When Privileged Access Manager is stopped, access rights to the database files are determined by native Windows permissions. Permissions are inherited from the parent directory in which Privileged Access Manager is installed. Because of this inheritance, the default access to the database files is read when Privileged Access Manager is stopped.

To protect Privileged Access Manager when it is stopped, you can change the Windows permissions for the database files to suit your enterprise requirements. Before you change the permissions, consider the following:

- The NT AUTHORITY\System user *must* have Windows permissions to read and write to the database files. The Privileged Access Manager authorization engine inherits privileges from the NT AUTHORITY\System user. If this user cannot access the database, the engine does not have sufficient native privileges to update the database.
- Users who need read and write access to Privileged Access Manager when it is stopped must have Windows permissions to read and write to the database files. Users who need read and write access include users who back up, restore, or upgrade Privileged Access Manager.
- Users that can use `selang` when Privileged Access Manager is stopped (`selang -l` option) must have the following permissions:
  - The ADMIN attribute or sub-administration privileges
  - Windows permissions to read and write to the database files
  - Windows permissions to change native repositories, if required
 For example, to use the config environment to change Privileged Access Manager registry entries when it is stopped, you must have sufficient Windows privileges to change the registry.

Only Privileged Access Manager administrators (users with the ADMIN attribute or with sub-administration privileges) can use `selang` to maintain the database when it is stopped. If the Privileged Access Manager administrators cannot access the database when it is stopped, no user can perform offline database maintenance and a deadlock may occur.

## Policy Model Database (Windows)

Managing tens or hundreds of databases individually is not practical. Privileged Access Manager supplies the Policy Model service, a component that lets you manage many databases from one central database. Using the Policy Model (PMD) service is optional, but it greatly simplifies administration at large sites.

#### NOTE

In Windows Task Manager, the Policy Model service appears as `sepmdd.exe`.

The Policy Model service uses a Policy Model database (PMDB). Like other Privileged Access Manager databases, the PMDB contains users, groups, protected resources, and rules governing access to the resources. In addition, the PMDB contains a list of *subscriber* databases. Each subscriber is a Privileged Access Manager database that resides on a separate computer, or another PMDB that resides on the same or another computer. A PMDB that updates a subscriber is the *parent* of the subscriber.



The PMDB is a useful tool for managing many databases that have similar authority restrictions and access rules.

Policy Model names are case-sensitive on Windows for compatibility with UNIX. When specifying PMDB names in commands, ensure that you use the correct case. The first character for a PMDB name consists of the alphanumeric characters "-" and "\_".

#### NOTE

You cannot use non-English characters in PMDB and host names.

#### NOTE

Although PMDB names are case-sensitive, you cannot have two PMDBs on the same computer with only the letter case being different. Privileged Access Manager uses the PMDB name as part of the file path but Windows is case-insensitive and so does not permit this. For example, myPMDB and MYpmdb are two different Policy Model databases but cannot live on the same system.

#### NOTE

For information about administering a PMDB (sepmcmd utility), see the *Reference Guide*. For information about managing PMDBs remotely using selang, see the *selang Reference Guide*.

### **PMDB Location on Disk**

All PMDBs on a computer reside in a common directory. The `_pmd_directory_` value in the following subkey of the Windows registry specifies the name of the directory:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd
```

The default value of `_pmd_directory_` in the NTFS root directory is: `ACInstallDir\data`, where `ACInstallDir` is the directory where you installed Privileged Access Manager (by default `C:\Program Files\CA\AccessControl`).

Each PMDB occupies a subdirectory in the common directory. The files in the subdirectory contain all the data that is required to define the Policy Model. Policy Model configuration settings are stored in a `Pmd` subkey of the Privileged Access Manager registry settings. The name of the subkey is the name of the Policy Model.

### **Managing Local PMDBs**

Privileged Access Manager offers a utility for administering PMDBs:

- **sepmcmd**  
A PMDB administration utility that lets you:
  - Administer subscribers
  - Truncate the update file
  - Administer Dual Control
  - Manage the Policy Model log file
  - Perform other administrative tasks

#### NOTE

For more details about `sepmcmd`, see the *Reference Guide*.

### **Managing Remote PMDBs**

Privileged Access Manager also offers you a range of `selang` commands that you can use in the `pmd` environment. These commands let you manage PMDBs remotely:

- **backuppmd**  
Backs up a PMDB.
- **createpmd**

Creates a PMDB.

- **deletepmd**  
Deletes a PMDB.
- **findpmd**  
Displays the names of all PMDBs on the computer.
- **listpmd**  
Lists the following information about a PMDB:
  - Subscribers and their status
  - PMDB description and its status
  - Commands in the update file and their offsets
  - Contents of the error log
- **pmd**  
A PMDB administration command that lets you:
  - Remove a subscriber from the list of unavailable subscribers
  - Clear the Policy Model error log
  - Start and stop the Policy Model service
  - Lock and unlock the Policy Model
  - Truncate the update file
- **restorepmd**  
Restores a PMDB from its backup files.
- **subs**  
A PMDB subscription command that lets you:
  - Add an existing subscriber to a parent PMDB
  - Add a new subscriber to a parent PMDB
  - Assign a parent PMDB to a database (Privileged Access Manager or another PMDB)
- **subspmd**  
Assigns a parent PMDB to the local database.
- **unsubs**  
Removes a subscriber from the PMDB.

**Note:** For a comprehensive explanation of *selang* commands you can use in the *pmd* environment, see the *selang Reference Guide*.

### **Architecture Dependency**

When deploying Privileged Access Manager, consider the hierarchy of your environment. At many sites, the network includes various architectures. Some policy rules, such as the list of trusted programs, are architecture-dependent. On the other hand, most rules are independent of the architecture of the system.

You can cover both kinds of rules by using a hierarchy. You can define a global database for architecture-independent rules, and can give it subscriber PMDBs that define architecture-dependent rules.

#### **NOTE**

The root PMDB and all its subscribers can reside on the same computer or on separate computers, depending on the physical needs of your environment.

### **Example: A Two-Tiered Deployment Hierarchy**

The following UNIX example also applies to a Windows architecture with small modifications.

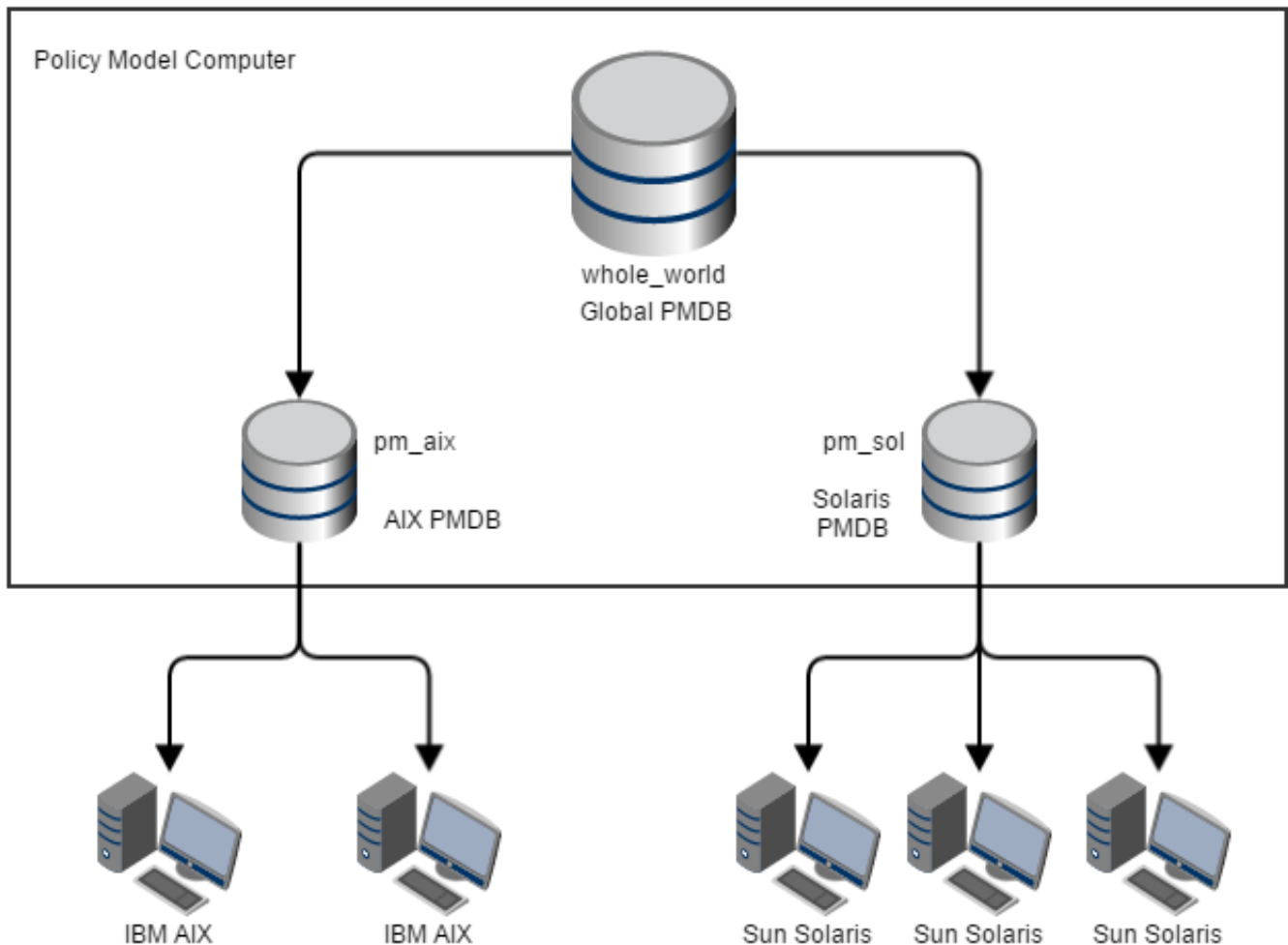
In the example, the site consists of IBM AIX and Sun Solaris systems. Because the list of trusted programs on IBM AIX differs from the one on Sun Solaris, the PMDBs need to consider architecture dependency.

To set up a multiple-architecture PMDB, set up your PMDBs as follows:

1. Define a PMDB named `whole_world`, to contain the users, groups, and all other architecture independent policies.
2. Define a PMDB named `pm_aix`, to contain all the IBM AIX-specific rules.
3. Define the PMDB `pm_sol` to contain all the Sun Solaris specific rules.

The PMDBs `pm_aix` and `pm_solaris` are subscribers of the PMDB `whole_world`. All IBM AIX computers at the site are subscribers of `pm_aix`. All Sun Solaris computers at the site are subscribers of `pm_sol`. The concept is illustrated in the following chart.

**Figure 51: Architecture\_Dependency**



4. When you enter platform-independent commands in `whole_world`, such as adding a user or setting a SURROGATE rule, all databases at the site are automatically updated.
5. When you add a trusted program to `pm_aix`, only IBM AIX computers are updated, without affecting the Sun Solaris systems.

### **Methods for Centrally Managing Policies**

Privileged Access Manager lets you manage several databases from a single computer in the following ways:

- **Automatic rule-based policy updates:** Regular rules that you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.

**NOTE**

Dual control is only available with this method and on UNIX only. Information about dual control for automatic rule-based policy updates is found in the *Endpoint Administration Guide for UNIX*. Information about automatic rule-based policy updates can also be found in the *Endpoint Administration Guide for Windows*.

- **Advanced policy management:** Policies (groups of rules) you deploy are propagated to all databases based on host or host group assignment. You can also undeploy (remove) policies and view deployment status and deployment deviation. Install and configure extra components to use this functionality.

**NOTE**

Information about advanced policy management is found in the *Enterprise Administration Guide*.

## Automatic Rule-based Policy Updates

Single-rule policy updates (regular selang rules) you make in a central database are automatically propagated to the subscriber databases. By subscribing several computers to the same database, and by subscribing one database to another, you can create a hierarchy. You configure your environment for automatic rule-based policy updates after installation.

**NOTE**

This method of managing policies is limited to letting you make single-rule policy updates across your hierarchy. Other functionality is only available through implementing advanced policy management and reporting.

### How Automatic Rule-Based Policy Updates Work

When you configure your environment for automatic rule-based policy updates, each rule you define in the central database is automatically propagated to all its subscribers in the following way:

1. A rule is defined for any PMDB with at least one subscriber.
2. The PMDB sends the command to all subscriber databases.
3. The subscriber database applies the propagated command.
  - a. If the subscriber database does not respond, the PMDB sends the command at a regular interval (by default, every 30 minutes) until the subscriber database has been updated.
  - b. If a subscriber database is responding, but refuses to apply the command, the PMDB places the command in the [Policy Model error log](#).
4. If the subscriber database is a parent to other subscribers, it then sends the command to its subscribers.

### **Example: Removing a user from all computers in a hierarchy**

If a user is deleted from a PMDB using the `rmusr` command, the same `rmusr` command is sent to all the subscriber databases. In this way, a single `rmusr` command can remove a user from many databases on various computers.

### How You Use a PMDB to Propagate Configuration Settings

When you edit a Policy Model's configuration, the new configuration values are propagated to the Policy Model's subscribers.

The following process describes how configuration updates are propagated to a Policy Model's subscribers:

1. You edit one or more of the Policy Model's configuration values.
2. The Policy Model writes the new configuration values to the virtual configuration file.

**NOTE**

The virtual configuration file does not contain values for the `audit.cfg` file. The Policy Model does not write any changes you make to this file to the virtual configuration file.

3. The Policy Model sends the new configuration values to its subscribers.

4. `selang` commands update each subscriber with the new configuration values.

### **Virtual Configuration File**

Each Policy Model has a virtual configuration file that contains the configuration values for its subscribers. The virtual configuration file is located in the PMD directory, and is named `cfg_configname`, where *configname* is the name of the Policy Model configuration.

The virtual configuration file does not contain the configuration values held in the `audit.cfg` file.

### **How New Subscribers Are Configured**

The Policy Model configures each new subscriber with the existing configuration values. The existing configuration values are stored in the virtual configuration file.

#### **NOTE**

The virtual configuration file does not store configuration values from the `audit.cfg` file. Any changes you make to the `audit.cfg` file prior to creating a new subscriber are not propagated to the new subscriber.

The following process describes how a Policy Model configures new subscribers:

1. You create a new subscriber to the Policy Model.
2. The Policy Model reads the values in its virtual configuration file.
3. The Policy Model adds the configuration values from its virtual configuration file to the `updates.dat` file. The `updates.dat` file also contains the access rules for the Policy.
4. The Policy Model sends the `updates.dat` file to the new subscriber.
5. `selang` commands configure the new subscriber with the values in the `updates.dat` file.

### **How You Can Set up a Hierarchy**

Privileged Access Manager uses the Policy Model service to propagate rule-based policy updates across the configured hierarchy. By subscribing several Privileged Access Manager computers to the same PMDB, and by subscribing one PMDB to another, you create a hierarchy.

The most straightforward way to set up the PMDB hierarchy is as you install Privileged Access Manager, so it is worth thinking through how you want to structure the hierarchy before you begin the installation. Ensure that all the hosts in the PMDB hierarchy are part of the same network. The parent PMDB and its subscribers must be able to communicate with each other. The parent must be able to connect with each of its subscribers by name, and every subscriber must be able to connect to the parent PMDB by name.

**Note:** For more information about installing Privileged Access Manager, see the *Implementation Guide*.

If you want to change the configuration that you created during installation or if you did not create a PMDB structure during installation, you can change or create the PMDB configuration at any time. You can do this in one of the following ways:

- With Privileged Access Manager Endpoint Management
- With the `sepmdb` utility

To create a PMDB hierarchy and enable automatic rule-based policy updates after installation, follow these steps:

1. Create and configure the master PMDB.
2. (Optional) Create and configure subscriber PMDBs.
3. Define parent PMDBs for the subscribing computers, named *endpoints*.

## Update Subscribers

When updating subscribers, the Policy Model performs the following actions:

1. The Policy Model tries to fully qualify subscriber names as they are added or deleted from the Policy Model.
2. The PMDB service, sepmdd, attempts to update a subscriber database.
3. If the maximum time elapses and the service does not succeed in updating a subscriber, it skips that particular subscriber and tries to update the rest of the subscribers on its list.
4. After it completes its first scan of the subscriber list, sepmdd then performs a second scan, in which it tries to update the subscribers that it did not succeed in updating during its first scan.

### NOTE

Whenever a PMDB encounters an error while propagating updates to subscribers, the sepmdd service creates an entry in the [Policy Model error log file](#). This file, ERROR\_LOG, is located in the [PMDB directory](#).

## Update a Policy Model Database

Working at the computer where the PMDB resides does not automatically update the PMDB itself. To update a PMDB, you need to specify it as your target database.

You can specify the PMDB using selang or Privileged Access Manager Endpoint Management. To specify a target database using selang, use the hosts command in the selang command shell:

```
hosts pmd_name@pmd_host
```

All selang commands now update the policy model database specified. The commands then automatically propagate to the active databases on this computer and of all subscriber computers.

### Example: Specify a target PMDB

To set the target database to policy1 on myPMD\_host, use the following command:

```
hosts policy1@myPMD_host
```

If you now enter the newusr command, the new user is added to the policy1 database as well as the active databases on this computer and of all subscriber computers.

## Clean Up the Update File

The sepmdd utility automatically writes each update it receives in the updates.dat file. To prevent the file from growing too large, we recommend that you delete processed updates from the file periodically.

To clean up the update file, use the following command:

```
sepmdd -t pmdbName auto
```

sepmdd calculates the offset of the first update entry that has not been propagated and deletes all the update entries before it.

### NOTE

For more information about sepmdd utility, see the *Reference Guide*.

## Propagate and Synchronize Passwords

Once you set up a PMDB hierarchy, you can use it to keep user passwords synchronized throughout your system when the user passwords are changed with the Windows User Manager or software other than Privileged Access Manager.

### NOTE

Privileged Access Manager also supports mainframe password synchronization.

**Follow these steps:**

1. Create a PMDB Hierarchy.
2. Enter the name of the appropriate parent PMDB as the passwd\_pmd entry value in the registry on every station on which users or administrators may change passwords.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl\passwd_pmd
```

The PMDB then propagates the password change to all its subscribers.

**NOTE**

If the PMDB sends a user password to a subscriber in which the user is not defined, settings are not changed and the user remains undefined for the subscriber.

**Remove a Subscriber**

If you no longer want to propagate updates to a particular subscriber, you should remove it.

**To remove a subscriber**

1. Remove the computer from the subscription list:

```
secmd -u PMDB_namecomputer_name
```

The computer is removed from the Policy Model subscription list.

2. Shut down seosd on the computer that you removed from the subscription list:

```
secons -s
```

The seosd service is shut down.

3. Delete the value of the parent\_pmd registry value in the following registry key on the computer you removed from the subscription list:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl
```

The computer will stop accepting updates from the parent PMDB.

4. Restart seosd.

The active database on the computer that you removed from the subscription list, is no longer a subscriber of the specified PMDB.

**NOTE**

Once the database is unsubscribed from the PMDB, the PMDB no longer sends commands.

**Filter Updates**

If you want your PMDB to update different subsets of data at different subscriber databases, you need to define which records are sent to subscriber databases.

**To filter updates:**

1. Configure PMDBs to serve as parents to subsets of subscribers.
2. Modify the *Filter* registry entry in the registry key of the parent PMDB, to point to a filter file you set up on the same computer.  
Updates to the subscriber databases are then limited to the records that pass the filter.

**Policy Model Filter File**

A filter file consists of lines, each with six fields. The fields contain information on:

- The form of access permitted or denied.  
For example, EDIT or MODIFY
- The environment affected.

For example, AC or native

- The class of the record.  
For example, USER or TERMINAL
- The objects, within the class, that the rule covers.  
For example, User1, AuditGroup, or COM2
- The properties that the record grants or cancels.  
For example, OWNER and FULL\_NAME in the filter line means that any command having those properties is filtered.  
You must enter each property exactly as it appears in the *Reference Guide*.
- Whether such records should be forwarded to the subscriber database or not:  
PASS or NOPASS

The following rules apply to each line in the filter file:

- You can use an asterisk (\*) to denote all possible values in any field.
- If more than one line covers the same records, the *first* applicable line is used.
- Spaces separate the fields.
- In fields with more than one value, semicolons separate the values.
- Lines beginning with # are considered a comment line.
- Empty lines are not allowed.

### Example: Filter file

The following example describes a line from a filter file:

|                |             |       |                      |                    |           |
|----------------|-------------|-------|----------------------|--------------------|-----------|
| CREATE         | AC          | USER  | *                    | FULL_NAME;OBJ_TYPE | NOPASS    |
| form of access | environment | class | record name( * =all) | properties         | treatment |

In this example, if we name the file with this line Printer1\_Filter.flt and edit the registry for PMDB PM-1 so that filter=C:\Program Files\CA\AccessControl\Printer1\_Filter.flt, then PMDB PM-1 will not propagate to its subscribers any records that create new users with the FULL\_NAME and OBJ\_TYPE property.

### Policy Model Error Log File

The Policy Model error log, which is organized chronologically, looks similar to this:

| Error Text                                                                                                                                                                           | Error Category       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <pre>20 Nov 03 11:56:07 (pmdbl): fargo nu u5 0 Retry ERROR: Login procedure failed (10068) ERROR: Cannot accept update from a non-parent PMDB (pmdbl@name.company.com) (10104)</pre> | Configuration Errors |
| <pre>20 Nov 03 19:53:17 (pmdbl): fargo nu u5 0 Retry ERROR: Connection failed (10071) Host is unreachable (12296)</pre>                                                              | Connection Errors    |



|                                                                                                                                                                                                                                        |                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <pre>20 Nov 03 11:57:06 (pmdbl): fargo nu u5 560 Cont ERROR: Failed to create USER u5 (10028) Already exists (-9)  20 Nov 03 11:57:06 (pmdbl): fargo nu u5 1120 Cont ERROR: Failed to create USER u5 (10028) Already exists (-9)</pre> | Database Update Errors |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|

The Policy Model error log is in binary format; you can view it only by entering the following command:

```
ACInstallDir/bin sepmd -e pmdname
```

#### NOTE

Do not manually delete an error log (for example, with the UNIX `rm` command). To delete the log, only use the following command:

```
ACInstallDir/bin sepmd -c pmdname
```

#### WARNING

The error log in Privileged Access Manager r5.1 and later versions has a format that is not compatible with the format of earlier versions. `sepmd` cannot handle error logs from these earlier versions. When you upgrade to a version that has this format, the old error log is copied to `ERROR_LOG.bak`; a new log file is created when you start `sepmd`.

#### Example: PMDB Update Error Message

The following example shows a typical error message:

```

date      time      pmdb name      subscriber      command      offset      flag
  ↓           ↓           ↓           ↓           ↓           ↓           ↓
20 Nov 03 19:53:17 (pmdbl): fargo nu u5 0 Retry
ERROR: Connection failed (10071) ← major level (type of error)
Host is unreachable (12296) ← minor level (cause of error)
                        ↑
                    return code

```

- The top line always consists of the date, time, and subscriber. The command that generated the error appears next, followed by the offset (in decimal format), which indicates the location of the failed update inside the updates file. Lastly, the flag indicates whether the PMDB retries the update automatically or continues without it.
- The second line shows an example of a major level message (what type of error occurred) and its return code.
- The third line displays an example of a minor level message (why the error occurred), and its return code.

#### Example: Error Message

A command may generate and display more than one error. Also, an error may consist of a major level message, a minor level message, or both.

The following error has only one message level:

```
Fri Dec 29 10:30:43 2003 CIMV_PROD:Release failed. Return code = 9241
```

This message occurs when `sepmd` pull attempts to release a subscriber that is already available.

## Native Policy Model Repositories

You can store all native environment user and group object types in the PMDB. By storing this information in the PMDB, you can receive information about objects using show commands (such as show user or show group). The returned objects are an image of the actual objects that are defined in Windows or UNIX subscribers.

After connecting to a Policy Model, a user can choose the following environments:

- AC
- Native
- NT
- UNIX
- Config

### NOTE

Native operates exactly as Windows while you are working in a Windows operating system, or exactly as UNIX while you are working on a UNIX operating system.

To use native environment repositories, use the following commands:

- Enter the following commands at the selang prompt:

```
env NT; find
```

Your results list all the native environment object types.

### NOTE

For descriptions of these object types, see the Windows environment classes and properties in the *Reference Guide*.

- Enter the following commands to receive a list of NT and Active Directory USER properties:

```
env NT; ruler user
```

- Enter the following commands to receive a list of NT and Active Directory GROUP properties:

```
env NT; ruler group
```

If a Policy Model is a subscriber of another (parent) Policy Model, it receives data from a parent through propagation and saves in the database all user and group properties, so you can see them and change them.

### NOTE

For more information, see the sepmd utility in the *Reference Guide*.

## Mainframe Password Synchronization

Privileged Access Manager supports password synchronization among mainframes running CA Top Secret, CA ACF2, or RACF security products (and CA Common Services CAICCI package) and Windows or UNIX computers running Privileged Access Manager. Synchronization is accomplished using the standard Privileged Access Manager password Policy Model method.

Any password change a mainframe user makes is propagated to all the machines in the password Policy Model hierarchy.

### Mainframe Password Synchronization Prerequisite

To work with Mainframe Password Synchronization on the server that has TNG/TND/NSM installed, Privileged Access Manager requires a prerequisite TNG/TND/NSM fix: T129430. Please contact support for getting the fix.

## Toggle Driver Interception

You can activate or deactivate the interception of the Privileged Access Manager filter driver.

**NOTE**

When the interception is deactivated, Privileged Access Manager protection that is not enforced by the filter driver still applies. This includes password quality checks, login events, Windows services events, STOP, and so on.

To activate interception, set UseFsiDrv to 1; to deactivate, set UseFsiDrv to 0.

You can find this configuration setting in the AccessControl section of the Privileged Access Manager registry.

After you change this registry value, restart Privileged Access Manager services.

## Disable CA Privileged Access Manager Server Control Kernel Interceptions

You can disable the following Privileged Access Manager interceptions at the kernel level:

- network interception
- process interception
- registry interception
- file interception

Even when the network, process, registry, and file classes are disabled and you are not using those classes to intercept kernel activity, the network, process, registry, and file interception processing code is initiated at boot time and working at run time, affecting performance. To improve performance, you can disable one or more interceptions from initiating at boot time.

### To disable Privileged Access Manager interceptions at the kernel level

1. Create one or more of the following registry entries of type REG\_DWORD and set the value of one or more entries to 1.
  - DisableNetworkInterceptiondisables network interception.
  - DisableProcessInterceptiondisables process interception.
  - DisableRegistryInterceptiondisables registry interception.
  - DisableFileInterceptiondisables file interception.

The entries must be created under the following registry key:

`HKLM\SYSTEM\CurrentControlSet\Services\drveng\Parameters`

2. Reboot the computer.  
Privileged Access Manager reloads without initializing the disabled interception types.

## Stack Overflow Protection

Stack Overflow Protection (STOP) is a feature that prevents hackers from creating and exploiting stack overflow to break into systems. Stack overflow enables hackers to execute arbitrary commands on remote or local systems, many times as the administrator. They do this by exploiting bugs in the operating system or other programs. These special types of bugs permit users to overwrite the program stack, changing the next command to be executed.

STOP works by intercepting crucial operating system calls to each application on the computer. Each call is then given an initial analysis before being sent for further analysis if it seems suspicious. Further analysis is performed using data from the STOP configuration and signature files.

### Enable STOP

STOP lets you prevent hackers from creating and exploiting stack overflow to break into your systems. You can enable STOP when installing Privileged Access Manager. Alternatively, you can enable STOP manually.

**To enable STOP:**

1. Enter the following command:

```
secons -s
```

Privileged Access Manager shuts down.

2. Set the *STOP OperationMode* registry entry to 1.  
The registry entry can be found in the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\StopPlg
```

When Privileged Access Manager is started, STOP modules will load and STOP will be enabled on the computer.

3. (Optional) Adjust STOP configuration using registry entries in the following keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\StopPlg
```

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\STOP
```

**NOTE**

For more information about STOP registry settings, see the *Reference Guide*.

4. Start Privileged Access Manager by entering the following command:

```
seosd -start
```

Privileged Access Manager starts up.

**Configure STOP for Receiving Signature File Updates**

You can make sure that all computers in your environment have the latest STOP information required for preventing stack overflow. You can do this by updating the STOP signature file on a central computer and setting up your computers to regularly retrieve the file.

**To configure STOP for receiving signature file updates**

1. Enter the following command:

```
secons -s
```

Privileged Access Manager shuts down.

2. Set the *STOPSignatureBrokerName* registry entry to the host name the computer you want to Privileged Access Manager to retrieve the signature file from.  
The registry entry can be found in the following key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\STOP
```

When you start Privileged Access Manager (and then at a defined interval), it retrieves the STOP signature file from the specified computer.

3. Set the *STOPUpdateInterval* registry entry to the interval at which you want the signature file updated.  
Privileged Access Manager retrieves the signature file from the specified computer at the specified interval.
4. (Optional) Adjust STOP configuration using registry entries in the following key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\STOP
```

**NOTE**

For more information about STOP registry settings, see the *Reference Guide*.

5. Start Privileged Access Manager by entering the following command:

```
seosd -start
```

Privileged Access Manager starts up.

**NOTE**

You can retrieve the signature file from any host using the eACSigUpdate utility. For more information about this utility, see the *Reference Guide*.

## Configure Settings

Privileged Access Manager lets you manage endpoint configuration settings remotely using Privileged Access Manager Endpoint Management or the selang config environment.

### Configuration Settings

Privileged Access Manager stores endpoint and Policy Model configuration settings it uses in:

- The Windows registry on Windows computers
- Initialization files (.ini) on UNIX computers

#### **NOTE**

For information about the configuration settings you can make and what they mean, see the *Reference section*.

### Change Configuration Settings

To affect how Privileged Access Manager and any Policy Models work, change the configuration settings.

#### **Follow these steps:**

1. In Privileged Access Manager Endpoint Management, do as follows:
  - a. Click Configuration.
  - b. Click Remote Configuration.
 The Remote Configuration page appears.
2. In the Remote Configuration Sections pane on the left, expand the configuration tree as required to reveal the section that contains the configuration setting you want to modify, then click that section.  
The Section: *sectionName* System Tokens page appears, displaying all the configuration settings in it.
3. Locate and edit the configuration settings as required, then click Save Tokens.  
The changed configuration setting is saved.

### Change Audit Configuration Settings

To affect how Privileged Access Manager generates and stores audit records, change the settings in the audit configuration files. You use selang commands to change the settings in the audit configuration files.

#### **Follow these steps:**

1. (Optional) If you are using selang to connect to a remote host, connect to the host using the following command:  
`host host_name`
2. Move to the config environment using the following command:  
`env config`
3. Use the editres config command to modify the configuration settings as required.  
The audit configuration settings are changed.

#### **Example: Modify Audit Configuration File**

The following example adds a line to the audit configuration file:

```
er CONFIG audit.cfg line+("FILE;*;Administrator;*;R;P")
```

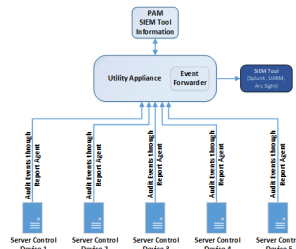
## Track User Behavior Activities on Server Control Endpoints Using an SIEM Tool

To track all activity and events performed on your Server Control endpoints (devices) for IT governance purposes, configure PAM to report them to a *Security information and Event Management (SIEM)* tool such as Splunk or ArcSight

The following diagram illustrates the typical SIEM architecture, including these important components:

- The Report Agent is a service that exists on all the Server Control endpoints. The Reporting Agent feeds all the events/activities performed on each Server Control Device to the Utility Appliance.
- The Utility Appliance collects and stores all the events that are performed on all the Server Control endpoints.
- The Event Forwarder is a service that helps to track all the activities/events performed on all the Server Control endpoints. These events are viewed in a third-party tool such as Splunk, CA UARM, Arc sight, or similar. The Event Forwarder is installed on the Utility Appliance.

**Figure 52: PAM SIEM Architecture**



To track all activity and events performed on your Server Control endpoints for IT governance purposes, configure PAM to report them to a *Security information and event management (SIEM)* tool such as Splunk or ArcSight

**To set up the SIEM tool and view reports:**

1. In the PAM UI, select **Configuration**, expand **Logs**, and then select **Syslog**. The **Syslog** panel appears.
2. Configure the following options:
  - a. Set the **Enable Syslog to the specified server** option.
  - b. Enter the IP address of the SIEM tool in the **Remote Server** field.
  - c. Enter the port number of the SIEM tool in the **Remote Port**; for example, 5141.
3. Select **Update** to commit your changes.
4. Configure the connection between the embedded endpoint and the Utility Server, using the following procedures:
  - a. Perform a few events on the endpoint to act as a resource.
  - b. Run the following command to stop the Access Control Services:

```
secons -sk
```

- c. Configure the Access Control Server settings using the appropriate procedures:

**For Windows:**

- a. In regedit, modify the following keys:
  - For Hkey\_Local\_Machine->Software->Computer Associates->Access Control->Common->Communication, edit the Distribution\_Server entry to point to the IP address of the Utility Server.
  - For Hkey\_Local\_Machine->Software->Computer Associates->Access Control->Report Agent, set the audit\_enabled entry to 1.
  - For Hkey\_Local\_Machine->Software->Computer Associates->Access Control->Report Agent, set the agent\_enabled entry to 1.
- b. Run the following command to set the password to N0tall0wed:

```
sechkey -t -pwd "N0tall0wed"
```

**For Linux:**

- a. Using a standard text editor such as vi, open the accommon.ini file. For PAM SC, the file resides in /opt/CA/PAMSCShared/. For PAM 12.8, the file resides in /opt/CA/AccessControlShared/.
- b. Modify the following flags:
  - Set reportagent\_enabled to 1.
  - Set Distribution\_Server to the IP address of the Utility Server.
  - Set audit\_enabled to 1.

- c. Run the following command to set the password to N0tall0wed:
 

```
seckey -t -pwd "N0tall0wed"
```
- d. Run the following command to start the Access Control Services:
 

```
seload
```
- e. Export the path by running the command. Use the appropriate library path for your implementation.
 

```
export LD_LIBRARY_PATH= /opt/CA/AccessControlShared/AccessControlShared/lib
```
5. Generate some audit events, to verify the SIEM integration. The following examples are for the Splunk UI.
  - a. Create a test file by running the command. Replace <student #> with a test value.
 

```
touch /work/file_splunk_<student #>
```
  - b. Go to selang and create an ACL. For example:
 

```
er file /work/file_splunk_<student #> defaces(none) owner(nobody)
```
  - c. Quit selang and try to access the file by running the following command. Replace <student #> with the appropriate value.
 

```
cat /work/file_splunk_<student #>
```
  - d. A permission denied message displays and the event is audited. Enter the following command to view the audit entry. Replace <student #> with the appropriate value.
 

```
Seaudit -a -st now-5 | grep "/work/file_splunk_<student #>"
```
  - e. Send the audit records to the SIEM tool using the following command:
 

```
/opt/CA/PAMDistServer/APMS/AccessControlShared/bin/ReportAgent -debug 0 -task 1
```
  - f. Log in to the Splunk UI and search for the events under **Search & Reporting**. Search for the name of the file that you used to generate the audit event. For example:
 

```
"/work/file_splunk_student1"
```

See the Splunk documentation for detailed procedures for your specific lab environments.

## Troubleshoot PAM SC

This content in this section describes how to troubleshoot PAM Server Control.

Use the table of contents to access the topics in this section.

### View Server Control Policy Deployment Audit Data

Use the **Deployment Audit** tab on the **Policies, Manage Server Control** page to view a descriptive list of Server Control policy deployment tasks. Each entry contains the following information (as applicable) about the associated deployment task:

To view the audit deployment tasks, follow these steps:

1. Log into the PAM UI using an account with the required privileges.
2. Navigate to **Policies, Manage Server Control**.
3. Select the **Deployment Audit** tab.

The **Deployment Audit** opens, displaying a sortable, filterable list of your policy deployment tasks. Each list entry contains the following information (as applicable):

- **Policy Name:** The name of the deployment task.
  - **Version:** The version of the deployment task.
  - **Device Name:** The device associated with the deployment task.
  - **Device Group:** The device group associated with the deployment task.
  - **Type:** The type of policy deployment task (one of Assign, Unassign, Upgrade, Downgrade, Device Group Deletion, Auto Assign, Direct Deploy, Direct Undeployed, Reset, or Restore)
  - **Status:** The status of the deployment task (one of Queued, Success, Failure, Warning, No Action, Prerequisite, Dependence, Fix, Already Assigned, Unknown)
  - **Comment:** Any selang output generated by the deployment task.
  - **Update Time:** The time at which the deployment task occurred
  - **Updated By:** The name of the administrator account that initiated the deployment task.
4. To view all the specifics of any deployment task in a dialog, select the associated entry in the list and select the View button.

## Troubleshoot Policies Deployed on Server Control Devices

This topic describes how to do the following operations to troubleshoot policies deployed on Server Control devices:

- [Troubleshoot policies deployed to Server Control devices](#)
- [Remove obsolete devices associated with uninstalled PAM Server Control Agents](#)

### Troubleshoot Policies Deployed to Server Control Devices

When you deploy a policy to a Server Control agent, the policy is not deployed on the assigned endpoint until policyfetcher retrieves the deployment task and runs the policy script. As a result, deployment errors can occur when the policy is transferred to or is deployed at the endpoint.

If such an error occurs, PAM provides the following troubleshooting actions to help you resolve the issue:

- **Redeploy Policies**  
Creates a deployment task that contains the policy script and deploys the task to the endpoint. Use this option when the policy deploys on the endpoint with errors, that is, the Selang policy script execution fails. Fix the command syntax of deploy or undeploy script manually before you can redeploy the policy.
- **Undeploy Policies**  
Undeploys a policy that was deployed on the endpoint successfully or with errors. For troubleshooting purposes, use this option when a policy deploys on an endpoint with errors and you want to remove the policy association with the device.
- **Reset Device**  
Resets an endpoint and undeploys all the effective policies on the specified host. Privileged Access Manager resets host status and deletes all GPOLICY, POLICY, and RULESET objects on the specified host by creating deployment tasks and sending the tasks to the host for execution.  
Use this option to clean an endpoint from all policy deployments and clean endpoint status.  
**NOTE**  
This option does not remove DEPLOYMENT or GDEPLOYMENT objects from the endpoint or from PAM, because you might need these objects for auditing purposes. After you reset an endpoint, you can assign policies to the endpoint as normal.
- **Restore Device**  
Undeploys any policies on the specified host, and then deploys all the policies that must be deployed (assigned or directly deployed) on the host by creating deployment tasks and sending the tasks to the host for execution. Use this option when you reinstall Server Control or the operating system on the endpoint, or when you restore an endpoint



from a backup, to redeploy all the policies that Server Control indicates are effective on that endpoint. This option does not change the endpoint status in PAM.

**To use the available troubleshooting actions, follow these steps:**

1. Log in to the PAM UI.
2. Navigate to the **Policies, Manage Server Control** panel.
3. Select the **Device Troubleshooting** tab.  
A sortable, filterable table of Server Control devices opens.
4. Select the entry for the device with an assigned policy that requires repair.
5. Optionally, to open a dialog containing details about the device including queued and assigned policies, select the **View** button.
6. To troubleshoot the policy that is assigned to the device, select the button that is associated with the troubleshooting action that you want to run (**Redeploy Policies**, **Undeployed Policies**, **Reset Device**, or **Restore Device**).

**NOTE**

You can also perform most of these actions using the [policydeploy utility](#).

**Remove Obsolete Devices Associated with Uninstalled PAM Server Control Agents**

When you uninstall a PAM Server Control Agent from a server, PAM does not automatically remove the device that is associated with that node. As a routine maintenance procedure, you should therefore remove these obsolete nodes from the PAM database.

**Follow these steps:**

1. Log in to the PAM UI.
2. Navigate to the **Devices, Manage Server Control** panel.
3. Select the entry for the PAM Server Control agent.
4. Select the **Delete** button.

**WARNING**

When you delete a node, Privileged Access Manager removes all the HNODE-related deployment tasks, removes all the deployment tasks packages (unless they have other deployment task members), then removes the HNODE object.

## Troubleshoot Policies Deployed on Server Control Device Groups

When you deploy a policy to a Server Control device group, the policy is not deployed on the group members until policyfetcher retrieves the deployment task and runs the policy script on each one. As a result, deployment errors can occur when the policy is being transferred to, or is being deployed at, any of the endpoints in the group.

If a deployment error occurs, PAM provides the following troubleshooting actions to help you resolve the issue:

- **Reset Device Group**

Resets the endpoints and undeploys all the effective policies on the hosts in the device group. PAM resets the host status and deletes all GPOLICY, POLICY, and RULESET objects on the hosts by creating deployment tasks and sending the tasks to the hosts for execution. Reset also removes device and device group associations.

Use this action to clean the endpoints in the group from all policy deployments.

**NOTE**

The reset device group action does not remove DEPLOYMENT or GDEPLOYMENT objects from the endpoint or from PAM, because you might need these objects for auditing purposes. After you reset an endpoint, you can assign policies to the endpoint as normal.

If you reset a PAM SC device group, PAM performs the following actions on all PAM SC devices in that group:

- Disassociates the PAM SC device from the PAM device.
- Creates a new PAM device that has a Server Control host but no Device Type set.
- Associates the disassociated PAM SC device with the newly created PAM device.
- Removes all device groups.
- Resets all device group policies and device policies.
- **Restore Device Group**  
Use the restore group action when you reinstall the PAM Server Control Agent or the operating system on the members of the device group members. Also use the restore group action to redeploy all the policies that are effective on members of the group when you restore an endpoint from a backup. This action does not change the endpoint status in PAM.  
The restore device group action performs the following tasks on each host in the device group:
  - a. Undeploys any policies on the specified host.
  - b. Deploys all the policies that must be deployed (assigned or directly deployed) on the host by creating deployment tasks.
  - c. Sends the tasks to the host for execution.

**To run the available troubleshooting actions, follow these steps:**

1. Log in to the PAM UI.
2. Navigate to the **Policies, Manage Server Control** panel.
3. Select the **Device Group Troubleshooting** tab.  
A sortable, filterable table of Server Control device groups opens.
4. Select the entry for the device group with an assigned policy that requires repair.
5. Optionally, to open a dialog containing details about the device group including its members, select the **View** button.
6. To troubleshoot the policy that is assigned to the device group, select the button that is associated with the troubleshooting action that you want to run (**Reset Device Group** or **Restore Device Group**).

## Troubleshoot Orphaned Data, Records, and Validation Errors

Orphaned data and records are possible with Policies, Policy Versions, Rulesets, and Deployments. Orphaned data and records usually occur if data and records that are inserted into the PIM Deployment Map Server using selang commands are not properly mapped among the entities (policies, rulesets, policy versions, deployments). Orphan records do not occur if they are inserted through the PIM User interface.

The following orphan types are possible:

- A Policy (GPOLICY) without a version (POLICY)
- A policy version (POLICY) without a Policy (GPOLICY)
- A Ruleset (RULESET) without a policy version (POLICY)
- A GDEPLOYMENT without a DEPLOYMENT
- A DEPLOYMENT without a GDEPLOYMENT

The utility identifies orphaned data and records that cannot be extracted until they are fixed on the PIM server, or that are analyzed and ignored. The utility displays the path to the JSON files that contain the orphan records. The Validate button is disabled, and a user cannot proceed with validation unless the errors are fixed or ignored.

To fix orphaned data or records, you can choose to correct or delete them on the PIM Server.

**To correct orphaned data or records:**

1. Check the console to find the paths of Orphan Policies, Orphan Rulesets, and Orphan Deployments at one of the following locations:

- <STAGINGLOCATION>\ExtractedData\6.OrphanPolicies.json
  - <STAGINGLOCATION>\ExtractedData\7.OrphanDeploymentsExt.json
  - <STAGINGLOCATION>\ExtractedData\8.OrphanRuleSets.json
2. Navigate to the paths and fix them.
  3. Re-run the utility to repeat the Extraction phase.

#### To delete orphaned data or records:

1. Check the console to find the paths of Orphan Policies, Orphan Rulesets, and Orphan Deployments at one of the following locations:
  - <STAGINGLOCATION>\ExtractedData\6.OrphanPolicies.json
  - <STAGINGLOCATION>\ExtractedData\7.OrphanDeploymentsExt.json
  - <STAGINGLOCATION>\ExtractedData\8.OrphanRuleSets.json
2. Navigate to the path <STAGING LOCATION>\ExtractedData\[OrphanFiles] and delete them if records are obsolete/unused and can be ignored.
3. Re-run the utility to repeat the Extraction phase. If the orphaned data or records are fixed, the utility lets you perform Validation directly.

After Validation, you may see the following issues and behaviors:

#### Validation Errors

To fix validation errors:

1. Navigate <STAGING LOCATION>\ExtractedData\error to find the errors.
2. Each error record mentions the error message. Review the reason for failure, and then review and fix the record in the JSON file.
3. Re-run the utility by clicking Start. The utility re-scans the data available in the Staging location.
4. Click Validate to re-validate the errors and finish the Validation phase.

#### Invalid Hosts

The utility identifies validation errors related to hosts during the Validation phase. If you think any of these hosts are invalid and can be ignored during migration, you can update the **invalidDevices.txt** file with all such invalid host names. You also must delete the corresponding JSON error from the validation hnode errors file named **1.HNodeExt.json**.

The utility will then ignore the records associated with the invalid hosts on re-validate, and lets the user proceed with further steps in the migration process.

The **invalidDevices.txt** file is located here:

```
<Migration Utility_INSTALL_PATH>/config
```

The **1.HNodeExt.json** file is located here:

```
<STAGING LOCATION>\ExtractedData\error
```

#### Follow these steps:

1. Update the **invalidDevices.txt** file with all such invalid host names.
2. Delete the corresponding JSON error from the validation host errors from the **1.HNodeExt.json** file.
3. Re-run the Migration Utility.

#### Invalid Host Groups

The utility identifies validation errors related to host groups during the Validation phase. If you think any of these host groups are invalid and can be ignored during migration, you can update the **invalidDeviceGroups.txt** file with all such invalid host group names. You also need to delete the corresponding error json from the validation Gnode errors file named **2.GHNodeExt.json**.

The utility will then ignore the records associated with the invalid host groups on re-validate, and lets the user proceed with further steps in the migration process.

The **invalidDeviceGroups.txt** file is located here:

`<Migration Utility_INSTALL_PATH>/config`

The **1.GHNodeExt.json** file is located here:

`<STAGING LOCATION>\ExtractedData\error`

**Follow these steps:**

1. Update the **invalidDeviceGroups.txt** file with all such invalid host group names.
2. Delete the corresponding JSON error from the validation host group errors from the **2.GHNodeExt.json** file.
3. Re-run the Migration Utility.

### **Invalid Policies**

The utility identifies validation errors related to policies during the Validation phase. If you think any of these policies are invalid and can be ignored during migration, you can update the **invalidpolicies.txt** file with all such invalid policy names. You also need to delete the corresponding error json from the validation errors file named **3.PolicyExt.json**.

The utility will then ignore the records associated with the invalid policies on re-validate, and lets the user proceed with further steps in the migration process.

The **invalidpolicies.txt** file is located here:

`<Migration Utility_INSTALL_PATH>/config`

The **3.PolicyExt.json** file is located here:

`<STAGING LOCATION>\ExtractedData\error`

**Follow these steps:**

1. Update the **invalidpolicies.txt** file with all such invalid policy names.
2. Delete the corresponding JSON error from the validation policy errors from the **3.PolicyExt.json** file.
3. Re-run the Migration Utility.

### **Invalid Deployment Data**

- No Trigger Name
- No Host Name or No Policy Name
- New Triggers

If the deployment contains invalid device or policy details, the invalid devices and invalid policies already appear in the **invaliddevices.txt** file under `<Migration Utility_INSTALL_PATH>/bin`. The migration ignores these deployments.

### **Invalid Users**

The utility identifies validation errors related to UNAB login policies when the user/group mentioned in the login policy is not present on PAM. If you think any of these users/groups are invalid and can be ignored during migration, you can update the **invalidusers.txt** file with all such invalid user/group names.

The migration utility will then create placeholder users for such invalid users/groups and migrate the login policies to PAM.

Post migration, to upgrade the migrated login policy, you need to delete the placeholder users and proceed with policy updates.

The migration utility creates the **invalidUsers.txt** file, located here:

`<Migration Utility_INSTALL_PATH>/config`

**Follow these steps:**

1. Update the **invalidUsers.txt** file with all such invalid host user/group names
2. Re-run the Migration Utility.

## Tune Performance

### MALLOC\_ARENA\_MAX=1 Not Working on Red Hat Linux 6.2

#### Valid on RedHat Linux 6.2

**Symptom:**

I noticed that the UNAB uxauthd agent process exceeds the permitted memory threshold and periodically restarts.

**Solution:**

The cause of the unstable behavior is related to the MALLOC\_ARENA\_MAX variable. To resolve the issue, do *one* of these procedures:

- Upgrade the glibc library.
- Set the memory threshold to 500-MB minimum:
  - Modify the agent\_vmemory\_max token value in uxauth.ini
  - Modify the ProcVSizeHigh token value in seos.ini if Privileged Access Manager is installed
- Decrease the number of used threads:
  - Modify the working\_threads token value in the uxauth.ini file to 2

### Performance Degrades When Privileged Access Manager Is Running

**Symptom:**

My computer slows when Privileged Access Manager is running. When I stop Privileged Access Manager, my computer performs as usual.

**Solution:**

To diagnose and correct the performance problem, [troubleshoot the performance problem](#).

### System Load on Privileged Access Manager Server Is Too High

**Symptom:**

I need to reduce system load on the Privileged Access Manager server.

**Solution:**

To reduce system load, do the following:

- Avoid deep hierarchies in the database.  
Deep hierarchies of users and resources require system loads to obtain and check all dependencies.
- Avoid generic rules for frequently used directories.  
If you define a generic rule for a frequently used directory, Privileged Access Manager checks many system actions. For example, if you write a generic protection rule that protects /usr/lib/\*, Privileged Access Manager checks every action in the system.
- (Solaris only) Specify that Privileged Access Manager bypasses file access checks when the file belongs to a process file system (/proc).

To specify that Privileged Access Manager bypasses file access checks when the file belongs to a process file system, verify that the value of the `proc_bypass` configuration setting is 1 in the `[SEOS_syscall]` section of the `seos.ini` file.

**Note:** For more information about `seos.ini` file tokens, see the *Reference* section.

## General UNAB Troubleshooting

This content describes how to perform general UNAB troubleshooting procedures.

### **Failed to Install UNAB**

#### **Symptom:**

I customized the installation package but when I attempt to install UNAB on the endpoint, the installation fails.

#### **Solution:**

Use the following procedure to troubleshoot the problem.

1. Review the UNAB installation log file, `uxauth_install.log` for errors. By default, the file is in the following directory:

```
/opt/CA/uxauth
```

2. Export the UNAB installation log file and send the file to CA Support.
3. Run the installation process in debug mode:
  - For native package installations, create a file that is named `seos_debug_on` in `/tmp` directory. Assign a debug level between 0-9 to the file.
4. Run the native package in debug mode:
  - AIX: Add `-e<log_file_name>` flag to the install command
  - HP-UX: Review the installation log file that the `swinstall` generates for `swjob`
  - Linux: Add `-vv` flag to the install command
  - Solaris: Add `-v` flag to the install command

### **Troubleshoot UNAB Registration**

The following section contains information that you can use to troubleshoot problems you encounter during UNAB registration with Active Directory.

#### ***UNAB Registration Failed Due to Incorrect Password***

##### **Symptom:**

When I try to register UNAB with Active Directory, registration fails with the following error message:

```
Preauthentication failed while getting initial credentials Kerberos preauthentication  
using <Administrator> failed
```

##### **Solution:**

UNAB registration failed due to an incorrect administrator password. To troubleshoot this issue, verify the administrator password and register UNAB.

#### ***UNAB Registration Failed Due to Incorrect Clock Skew***

##### **Symptom:**

When I try to register UNAB with Active Directory, I receive the following error message:

```
Clock skew too great while getting initial credentials Kerberos preauthentication using  
<Administrator> failed
```

**Solution:**

UNAB registration failed because the clock skew between Active Directory and the UNAB endpoint is larger than configured.

To resolve this issue, follow these steps:

1. Manually synchronize the UNAB endpoint clock with that of Active Directory.
2. Set `use_time_sync` token value to `yes` under the `[Agent]` section in `uxauth.ini` to configure time synchronization automatically.

***UNAB Registration Failed Due to Incorrect NTP Server Configuration*****Symptom:**

When I try to register UNAB with Active Directory, I receive the following error message:

```
WARNING: NTP service location is specified incorrectly
```

**Solution:**

The UNAB registration failed because the network time protocol server (NTP) is incorrectly configured.

To troubleshoot this issue, set the `ntp_server` token under the `[Agent]` section in `uxauth.ini` to point to the NTP server.

***UNAB Registration Failed Due to Invalid Configuration*****Symptom:**

When I try to register UNAB in Active Directory, I receive the following error message:

```
Error initializing Kerberos 5 library.Please check '/opt/CA/uxauth/uxauth.ini' Kerberos  
preauthentication using <Administrator> failed
```

***uxconsole -register Fails*****Valid on UNIX****Symptom:**

When I run `uxconsole -register` to register a UNAB endpoint, the following error message appears:

```
No server can be used as a DC for communicating with Active Directory.
```

```
Please check the lookup_dc_list and ignore_dc_list tokens in the [ad] section.
```

**Solution:**

When uxconsole registers the UNAB endpoint in Active Directory, the Active Directory site that is closest to the physical location of the endpoint is discovered. However, the ignore\_dc\_list configuration setting in the ad section of the uxauth.ini file lists domain controllers that the UNAB endpoint does not communicate with. If all domain controllers from the discovered Active Directory site are listed in the ignore\_dc\_list configuration setting, registration fails.

To fix this problem, delete the names of any domain controllers in the discovered Active Directory site from the ignore\_dc\_list configuration setting. Rerun the uxconsole utility.

**NOTE**

The uxconsole utility writes the name of the discovered Active Directory site to the ad\_site configuration setting in the ad section of the uxauth.ini file. For more information about UNAB Active Directory site support, see the *Implementation Guide*.

**UNAB Login Policy Not Distributed****Symptom:**

I attempted to deploy a UNAB login policy to the UNAB endpoints, but the policy is not distributed.

**Solution:**

To troubleshoot this issue, follow these steps:

1. Verify that UNAB is started on the endpoint:
  - a. Open a command prompt window on the endpoint.
  - b. Run the following command:

```
./uxauthd.sh status
```

A message informs you of the status of UNAB.

2. Verify that the policy was downloaded to the host:
  - a. From a command prompt window on the endpoint, run the following command:

```
./uxconsole -status -detail
```

The information includes the policy name, if deployed to the endpoint.

3. Review the policy authorization commands that the Enterprise Management Server sent to the UNAB endpoint.
  - From a command prompt window on the endpoint, run the following command:

```
./uxaudit -a
```

```
18 Jan 2011 11:03:23 S UPDATE          TERMINAL    ac_entm_pers  338 10 _default
      acmanager.forwardinc.com auth terminal _default xuid(yaeyu01)access(read) (OS
      user)
```

Verify that the rules were not modified.

4. Search the syslog file for Message Queue communication errors.
5. Verify the user account for login permissions and status.
6. Run the following command for a command prompt window:



```
uxconsole -manage -show -user <AD_user_account>
```

## **ReportAgent Fails to Send Reports to the Enterprise Management Server**

### **Symptom:**

I started UNAB and verified that the ReportAgent daemon is running but I cannot view reports in Privileged Access Manager Enterprise Management.

### **Solution:**

Use the following procedure to troubleshoot this issue:

1. Check the syslog for Message Queue server communication-related error messages in the 'UNAB EP communication problems with ENTM' section.
2. Verify that the audit\_enabled token under the [ReportAgent] section in the accommon.ini file is set to 1, if you want to send reports data to the Audit Log.
3. Enable ReportAgent debugging.
4. Set the debug token under the [ReportAgent] section in the accommon.ini file to 1
5. Review the UNAB reports debug file unab2xml.log. The file is located in the following directory:

```
/opt/CA/PAMSCShared/log
```

6. Run the ReportAgent manually to generate a UNAB database snapshot:

```
/opt/CA/PAMSCShared/bin/ReportAgent -debug 0 -task 2 -now
```

### **NOTE**

- Add the path '/opt/CA/PAMSCShared/lob' to \$LD\_LIBRARY\_PATH before you run the ReportAgent manually.
- Remove the .dat files from the /opt/CA/PAMSCShared/data/audit2txt/ directory before you manually run the ReportAgent.
- For more information about ReportAgent utility debug mode, refer to the *Reference Guide*.

## **Kerberos Preauthentication Fails When Registering a UNAB Host**

### **Valid on UNIX**

### **Symptom:**

When I use the uxconsole -register command, I receive the following error message:

```
krb5_set_config_files failed for /opt/CA/uxauth/uxauth.ini: Missing open brace in profile
```

```
Kerberos preauthentication using <Administrator> failed
```

### **Solution:**

There is an unset configuration setting in the uxauth.ini file. To fix this problem, verify that each configuration setting in the uxauth.ini file has a value.

**Receive Error Code 2803 When Registering or Starting UNAB****Valid on UNIX****Symptom:**

I receive the following error message when I try to register a UNAB host in Active Directory, or I try to start UNAB:

```
Unable to open nss or create nss cache. Error code 2803.
```

**Solution:**

Not enough memory exists in the /var directory. To fix this problem, verify that less than 95 percent of /var is used, and retry the command.

**Active Directory User Cannot Log in to UNAB Endpoint****Valid on UNIX****Symptom:**

An Active Directory user that has UNIX attributes cannot log in to a UNAB endpoint.

**Solution:**

To troubleshoot the problem, follow these steps:

1. Verify that the container of the user is one of the following:
  - The container that is specified in the user\_container configuration setting.
  - A sub-container under the container specified in the user\_container configuration setting.

**NOTE**

The user\_container configuration setting is located in the AD section of the uxauth.ini file.

2. Verify that the user has a UID and a GID in Active Directory.
3. Verify that the user is not suspended.
4. Verify that UNAB is started on the endpoint:
  - a. Open a command prompt window on the endpoint.
  - b. Run the following command:

```
./uxauthd.sh status
```

A message informs you of the status of UNAB.

5. Verify that the endpoint is registered in Active Directory.

**NOTE**

If the endpoint is not registered in Active Directory, use the uxconsole -register utility to register the host.

6. Stop the name or password caching daemon for your OS on the endpoint, as follows:
  - a. Stop UNAB:

```
./uxauthd.sh stop
```

- b. Delete the NSS cache database:

```
rm -rf /opt/CA/uxauth/etc/nss.db
```

- c. Check if the name or password caching daemon for your OS is running on the endpoint.  
For example, for a Linux or Solaris endpoint, check if the nscd daemon is running. For an HP-UX endpoint, check if the pwgrd daemon is running.
- d. If the name or password caching daemon for your OS is running, kill the process.
- e. Start UNAB:

```
./uxauthd.sh start
```

- 7. Obtain a Ticket Granting Ticket (TGT) using a different Active Directory user account.  
Run the following command to connect to Active Directory using the Administrator account:

```
./uxconsole -krb -init Administrator
```

#### NOTE

You can obtain a TGT using the agent keytab, for example:

```
./uxconsole -krb -init -k
```

- 8. Resolve the Active Directory user account directly:
  - Run the following search:

```
./uxconsole -ldap -search "(&(objectClass=user)(sAMAccountName=johndoe))"
```

Check for discrepancies between the expected and actual user account name.

- 9. Search for the user account in other domains, if applicable.
  - Run the following command:

```
./uxconsole -ldap -search -b DC=unabca,DC=test,DC=co,DC=il "(&(objectClass=user)
(objectCategory=person))"
```

- 10. Verify that the user account UNIX attributes are identical on the Active Directory and UNIX.

### **User Cannot Run Commands on a UNAB Endpoint**

#### **Symptom:**

I successfully log in to a UNAB endpoint, and UNAB creates a P (permitted) record in uxaudit, the UNAB audit file, that corresponds to my login. However, I cannot run any UNIX commands on the endpoint.

#### **Solution:**

The user has previously logged in to the same endpoint with the same username but with a different UID, so the user cannot access their /home directory.

To fix this problem, follow these steps:

- 1. Delete the /home directory for the user.

#### NOTE

The /home directory is often located at /home/userName.

- 2. Ask the user to log in to the endpoint.  
A new /home directory is created for the user. The user can now perform UNIX commands on the UNAB endpoint.

## **I Cannot View UNAB Endpoint in World View**

### **Valid on UNIX**

#### **Symptom:**

I use Privileged Access Manager Enterprise Management to manage UNAB endpoints, but a UNAB endpoint does not appear in World View.

#### **Solution:**

Verify that the UNAB endpoint can communicate with the Distribution Server. Do the following on the UNAB endpoint:

1. Verify that the value of the `Distribution_Server` configuration setting is set to the name of the Distribution Server computer.  
The `Distribution_Server` configuration setting is located in the communication section of the `accommon.ini` file.  
**Example:** `ssl://ds.comp.com:7243`  
**Note:** By default, the Utility Appliance is located on the Enterprise Management Server.
2. Verify that the Message Queue password is correct. The endpoint uses this password to communicate with the Utility Appliance. Do the following:
  - a. Open a command prompt window.
  - b. Run the following command:

```
acuxchkey -t pwd "password"
```

- *password*  
Defines the Message Queue password. By default, this password is the communication password that you define when you install Privileged Access Manager Enterprise Management.

3. Restart the UNAB agent, as follows:
  - a. Navigate to the UNAB `lbin` directory.  
By default, this directory is under `/opt/CA/uxauth`
  - b. Restart the UNAB agent:

```
./uxauthd.sh restart
```

4. Verify that the Message Queue server is running, as follows:
  - Windows: Verify that the PAM SC Message Queue service is running.
  - UNIX: Verify that the `tibemsd` process is running.
5. Check the syslog or event viewer for Message Queue server communication errors.
6. Set the Message Queue server to log communicated-related messages to a log file:
  - UNIX:
    - a. Open the `pmd.ini`.
    - b. Modify the `debug_mode` token in the `[endpoint_management]` section to 1.
  - Windows:
    - a. Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\ DMS_NAME  
  \endpoint_management
```

- b. Modify the `debug_mode` token value to 1

7. Restart the Enterprise Management Server to apply the changes. Review the endpoint\_management.log file located in the DMS directory for communication messages.
8. You have verified that the UNAB endpoint can communicate with the Utility Appliance.

### **I Cannot Start Daemons on Linux s390 Endpoint**

**Valid on Linux s390 and Linux s390x**

**Symptom:**

I cannot start the uxauthd or ReportAgent daemon.

**Solution:**

UNAB cannot locate the Java environment on the endpoint. To fix this problem, follow these steps:

1. Verify that the java\_home configuration setting in the global section of the accommon.ini file contains the path to the Java environment.
2. Set the value of the LD\_LIBRARY\_PATH environment variable to the path to the shared libraries of the Java environment.

### **User Cannot Log in or Change Password**

**Valid on UNIX**

**Symptom:**

When I try to log in or change my password on a UNAB endpoint, the following error message appears:

```
passwd: Authentication token manipulation error
```

**Solution:**

The PAM module timed out while waiting for uxauthd to respond to the password change request.

To fix this problem, follow these steps:

1. Increase the value of the pam\_receive\_timeout configuration setting in the pam section of the uxauth.ini file. For example, pam\_receive\_timeout=100
2. Stop and restart UNAB.

**NOTE**

For more information about the uxauth.ini file, see the *Reference Guide*.

**NOTICE**

For information about troubleshooting policies deployed on Server Control and UNAB devices and device groups, see the following topics:

- [Troubleshoot Policies Deployed on Server Control Devices](#)
- [Troubleshoot Policies Deployed on Server Control Device Groups](#)
- [Troubleshoot Policies Deployed on UNAB Devices](#)
- [Troubleshoot Policies Deployed on UNAB Device Groups](#)

## **Troubleshoot Policies Deployed on UNAB Devices**

When managing UNAB devices, discrepancies between the policies that are deployed on the PAM server and the UNAB devices can occur over time. These discrepancies are typically due to policy deployment failures, issues on the target

UNAB devices themselves, or both. If such discrepancies occur, PAM provides the following UNAB troubleshooting actions to help you resolve the issues:

- **Redeploy Policies**

Redeploys the specified UNAB (config and login authorization) policies on the specified UNAB device.

- **Undeploy Policies**

Undeploys a login authorization policy that was deployed on the specified UNAB device successfully or with errors. For troubleshooting purposes, use this option when the login authorization policy deploys on the endpoint with errors and you want to remove the policy association with the device.

- **Reset Device**

Resets the specified UNAB device. After you reset a UNAB device, you can reassign policies to that device as normal. If you reset a UNAB device, PAM performs the following actions:

- Disassociates the UNAB device from the PAM device.
- Creates a new PAM device that has a Server Control host but no Device Type set.
- Associates the disassociated UNAB device with the newly created PAM device.
- Removes all device and device group associations.
- Undeploys all the associated login authorization policies on that device.

- **Restore Device**

Undeploys all policies (assigned or directly deployed) on the specified host and then restores those policies. Use this option when you reinstall the UNAB Agent, reinstall the operating system on the endpoint, or when you restore an endpoint from a backup to redeploy all the policies that are effective on that endpoint.

**To use the available troubleshooting actions, follow these steps:**

1. Log in to the PAM UI.
2. Navigate to the **Policies, Manage UNAB Policies** panel.
3. Select the **Device Troubleshooting** tab.  
A sortable, filterable table of UNAB devices opens.
4. Select the entry for the device with an assigned policy that requires repair.
5. Optionally, to open a dialog containing details about the device including queued and assigned policies, select the **View** button.
6. To troubleshoot the policy that is assigned to the device, select the button that is associated with the troubleshooting action that you want to run (**Redeploy Policies**, **Undeploy Policies**, **Reset Device**, or **Restore Device**).

## Troubleshoot Policies Deployed on UNAB Device Groups

When managing UNAB devices in device groups, discrepancies between the policies that are deployed on the PAM server and the UNAB devices in the device groups can occur over time. These discrepancies are typically due to policy deployment failures, issues on the target UNAB devices themselves, or both. If such discrepancies occur, PAM provides the following UNAB troubleshooting actions to help you resolve the issues:

- **Reset Device Group**

Resets the UNAB devices in the specified device group. After you reset a UNAB device group, you can reassign policies to that group as normal.

If you reset a UNAB device group, PAM performs the following actions on all UNAB devices in that group:

- Disassociates the UNAB devices from the PAM device.
- Creates a new PAM device that has a Server Control host but no Device Type set.
- Associates the disassociated UNAB device with the newly created PAM device.
- Removes all device and device group associations.
- Undeploys all the associated login authorization policies on those devices.

- **Restore Device Group**

Use the restore device group action when you reinstall the UNAB Agent or to reinstall the operating system on members of the device group. Also use the restore device group action to redeploy all the policies assigned to members of the device group when you restore an endpoint from a backup. This action does not change the endpoint status in PAM.

The restore device group action performs the following tasks on each UNAB device in the device group:

- a. Undeploys any policies on the specified device.
- b. Redeploys all the (assigned or directly deployed) policies on the device.

**To run the available troubleshooting actions, follow these steps:**

1. Log in to the PAM UI.
2. Navigate to the **Policies, Manage UNAB Policies** panel.
3. Select the **Device Group Troubleshooting** tab.  
A sortable, filterable table of UNAB device groups opens.
4. Select the entry for the device group with an assigned policy that requires repair.
5. Optionally, to open a dialog containing details about the device group including its members, select the **View** button.
6. To troubleshoot the policy that is assigned to the device group, select the button that is associated with the troubleshooting action that you want to run (**Reset Device**, or **Restore Device Group**).

## Troubleshoot the Reporting Service

The topics that are discussed in this article help you troubleshoot the problems faced while working with the reporting service:

### Troubleshoot the Report Agent on a UNIX Computer

#### **Valid on UNIX**

The Report Agent collects scheduled snapshots of the local Privileged Access Manager database and any policy model databases (PMDBs) on the endpoint. The Report Server sends this snapshot in XML format to the report queue on the Utility Appliance.

#### **NOTE**

The Report Agent also performs other tasks. For more information about the Report Agent, see the *Reference facet*.

#### **To troubleshoot the Report Agent on a UNIX computer**

1. Verify that the library path environment variable is set correctly. Do the following actions:
  - a. su to root.
  - b. Set the library path environment variable to *ACSharedDir/lib*. By default, *ACSharedDir* is the following directory:

`/opt/CA/PAMSCShared`

- c. Export the library path environment variable.
2. Verify that the following configuration settings are correct. The configuration settings are located in the [ReportAgent] section of the accommon.ini file:

#### **NOTE**

You can use either Privileged Access Manager Endpoint Management or selang commands to verify the value of the configuration settings. However, for this procedure we recommend that you use selang commands in the config environment to change the value of configuration settings. Using selang commands lets you change the configuration settings in this procedure without having to stop and restart Privileged Access Manager.

– **reportagent\_enabled**

Specifies whether reporting is enabled (1) on the local computer.

**Default:** 0

**WARNING**

Set the value of this configuration setting to 1 to enable the Report Agent to run automatically. If the value of this configuration setting is 0, the Report Agent does not send scheduled snapshots of the database to the Utility Appliance. However, if the value of this configuration setting is 0 you can still run the Report Agent in debug mode.

– **schedule**

Defines the schedule of when reports are generated and sent to the Utility Appliance.

You specify this setting in the following format: time@day[,day2][...]

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

**Example:** "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

– **send\_queue**

Defines the name of the Message Queue on the Utility Appliance to which the Report Agent sends snapshots of the local database.

**Default:** queue/snapshots

**WARNING**

Do not change the default value of this configuration setting.

3. Verify that the following configuration setting is correct. The configuration setting is located in the [communication] section of the accommon.ini file:

**NOTE**

You can use either Privileged Access Manager Endpoint Management or selang commands to verify the value of the configuration settings. However, for this procedure we recommend that you use selang commands in the config environment to change the value of configuration settings. Using selang commands lets you change the configuration settings in this procedure without having to stop and restart Privileged Access Manager.

– **Distribution\_Server**

Defines the Utility Appliance URL.

**Default:** none

**Example:** ssl://172.24.176.145:61616 This URL configures the Report Agent to communicate with the Utility Appliance at the IP address 172.24.176.145 on port 61616, using the SSL protocol.

4. Verify that the following line exists in the [daemons] section of the seos.ini file:

```
ReportAgent = yes, ACSharedDir/lbin/report_agent.sh start
```

This line enables the Report Agent daemon to execute automatically when Privileged Access Manager starts.

**NOTE**

By default, the *ACSharedDir* directory is located at /opt/CA/PAMSCShared

5. Stop Privileged Access Manager:

```
secons -s
```

Privileged Access Manager and the Report Agent stops.

6. Navigate to the following directory:

```
ACSharedDir/bin
```



7. Run the Report Agent in debug mode, using the following command:

```
./ReportAgent -debug 0 -task 0 -now
```

- **ReportAgent**  
Runs the Report Agent.
  - **-debug 0**  
Specifies to run the Report Agent in debug mode and to display the output on the console.  
**Note:** You cannot run the Report Agent in debug mode if the Report Agent daemon is enabled.
  - **-task 0**  
Specifies that the Report Agent collects and sends information about the Privileged Access Manager database, and any local PMDBs, to the Utility Appliance. This information is used to generate reports.
  - **-now**  
Specifies to run the Report Agent now.
8. Review the Report Agent output as follows:
- Review the output for errors.
  - Verify that the correct names are specified in the Send Queue and the Report File parameters in the Send report parameters section.
9. Start Privileged Access Manager:

```
seload
```

Privileged Access Manager and the Report Agent start.

### Example: Report Agent Output

The following Report Agent output shows the Send Queue and Report File parameters:

```
-----
Send report parameters:
-----
Send Queue..... queue/snapshots
Report File..... /work/opt/CA/PAMSCShared/data/db2xml/ACDB.xml
-----
start sending report to queue 'queue/snapshots'...
```

### Troubleshoot the Report Agent on a Windows Computer

#### Valid on Windows

The Report Agent collects scheduled snapshots of the local Privileged Access Manager database and any policy model databases (PMDBs) on the endpoint. The Report Agent sends this snapshot in XML format to the report queue on the Utility Appliance.

**NOTE**

The Report Agent also performs other tasks. For more information about the Report Agent, see the *Reference facet*.

**To troubleshoot the Report Agent on a Windows computer**

1. Verify that the following configuration settings are correct. The configuration settings are located in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent
```

**NOTE**

You can use either Privileged Access Manager Endpoint Management or `selang` commands to verify the value of the configuration settings. However, for this procedure we recommend that you use `selang` commands in the config environment to change the value of configuration settings. Using `selang` commands lets you change the configuration settings in this procedure without having to stop and restart Privileged Access Manager.

- **reportagent\_enabled**

Specifies whether reporting is enabled (1) on the local computer.

**Default:** 0

**WARNING**

Set the value of this configuration setting to 1 to enable the Report Agent to run automatically. If the value of this configuration setting is 0, the Report Agent does not send scheduled snapshots of the database to the Utility Appliance. However, if the value of this configuration setting is 0 you can still run the Report Agent in debug mode.

- **schedule**

Defines the schedule of when reports are generated and sent to the Utility Appliance.

You specify this setting in the following format: `time@day[,day2][...]`

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

**Example:** "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

- **send\_queue**

Defines the name of the Message Queue on the Utility Appliance to which the Report Agent sends snapshots of the local database.

**Default:** queue/snapshots

**WARNING**

Do not change the default value of this configuration setting.

2. Verify that the following configuration setting is correct. The configuration setting is located in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communication
```

- **Distribution\_Server**

Defines the Utility Appliance URL.

**Default:** none

**Example:** `ssl://172.24.176.145:61616` This URL configures the Report Agent to communicate with the Utility Appliance at the IP address 172.24.176.145 on port 61616, using the SSL protocol.

3. Verify that the Privileged Access Manager Report Agent service is started.

**NOTE**

Set the `reportagent_enabled` configuration setting to 1 to configure the Privileged Access Manager Report Agent service to start automatically.

4. Open a command prompt window and stop Privileged Access Manager:

```
secsns -s
```

Privileged Access Manager stops, including the Report Agent service.

5. Run the Report Agent in debug mode, using the following command:

```
reportagent -debug 0 -task 0 -now
```

- **reportagent**  
Runs the Report Agent.
- **-debug 0**  
Specifies to run the Report Agent in debug mode and to display the output on the console.  
**Note:** You cannot run the Report Agent in debug mode if the Report Agent service is started.
- **-task 0**  
Specifies that the Report Agent collects and sends information about the Privileged Access Manager database, and any local PMDBs, to the Utility Appliance. This information is used to generate reports.
- **-now**  
Specifies to run the Report Agent now.

6. Review the Report Agent output as follows:

- Review the output for errors
- Verify that the correct names are specified in the Send Queue and the Report File parameters in the Send report parameters section

7. Start Privileged Access Manager:

```
seosd -start
```

Privileged Access Manager starts and the Report Agent service starts.

### Example: Report Agent Output

The following Report Agent output shows the Send Queue and Report File parameters:

```
-----
Send report parameters:
-----
Send Queue..... queue/snapshots
Report File..... C:\Program Files\CA\PAMSC\data\db2xml\ACDB.xml
-----
start sending report to queue 'queue/snapshots'...
```

### Library Path Environment Variable Example

The following example sets and exports the library path environment variable on a Linux or Solaris computer:

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/PAMSCShared/lib
export LD_LIBRARY_PATH
```

The following example sets and exports the library path environment variable on an AIX computer:

```
export LIBPATH=$LIBPATH:/opt/CA/PAMSCShared/lib
```

The following example sets and exports the library path environment variable on an HP-UX computer:

```
export SHLIB_PATH=$SHLIB_PATH:/opt/CA/PAMSCShared/lib
```

### **Troubleshoot the Utility Appliance**

On the Utility Appliance, the Message Queue receives information that the Report Agents send from the endpoints. Message-driven Java beans (MDBs) then read the data in the Message Queue and write the data to the central database.

#### **To troubleshoot the Utility Appliance:**

1. Log in to the ActiveMQ Web Administration Console. The default address is <https://<hostname>:8161/admin>

#### **NOTE**

The default port number is 8161. However, you can configure another value during the ActiveMQ installation.

2. Enter your username and password.

#### **NOTE**

The default username is admin. You can change the username during the ActiveMQ installation. You specify the password during the ActiveMQ installation.

3. Click Queues at the top of the page. A list of queues on the Utility Appliance appears.
4. Open a command prompt window on an endpoint.
5. (UNIX) Set the library path environment as in the following example:
  - a. su to root.
  - b. Set the library path environment variable to ACSharedDir/lib. By default, ACSharedDir is in the following directory:

```
/opt/CA/PAMSCShared
```

- c. Export the library path environment variable.
6. (UNIX) Navigate to the following directory: ACSharedDir/bin
  7. Run the Report Agent on the endpoint. Run one of the following commands:
    - a. Windows

```
ReportAgent -report snapshot
```

- b. UNIX

```
./ReportAgent -report snapshot
```

8. The Report Agent sends a snapshot of the Privileged Access Manager database and any local PMDBs to the report queue on the Utility Appliance.
9. Review the *queue/snapshots* queue and refresh the page after the Report Server runs. If the number of Messages Enqueued grows, but the number of Messages Dequeued does not grow, WildFly may not be running. Troubleshoot WildFly.

### **JasperReports Server Is Down or Unreachable**

#### **Symptom:**

When I try to view a report in Privileged Access Manager, I receive the following error message:

```
Fatal: Failed to execute CreateReportInstance. ERROR MESSAGE: Exception:Connection
refused: connect
```

#### **Solution:**

To troubleshoot this problem, check the following points:

1. Verify that you have configured a successful connection to the JasperReports Server. To verify the connection status, do the following steps:
  - a. Log in to Privileged Access Manager.
  - b. Navigate to **System, Connection Management, Report Server Configuration, Manage Connection**.
  - c. Ensure that you have provided correct values in the configuration fields.
  - d. Click **Submit**. If you receive an error message, then recheck your configuration values.
2. Ensure that the Tomcat service is running on the JasperReports Server.

### **Report Execution Hangs**

#### **Symptom:**

When I run a report in the Privileged Access Manager web interface, I observe the following behavior:

- The report status shows *Pending/Deleted* for a long time.
- The report data is missing even though the report status shows *Complete*.

To view the report status, navigate to *Reports, Tasks, View My Reports* in the web interface.

#### **Solution:**

The cardinality Estimator(CE) that comes with Microsoft SQL 2014 database degrades the performance when compared to the earlier databases. If CE negatively influences the critical workloads, disable its use by reverting to a database compatibility level below 120.

1. Navigate to your application database.
2. Right-click the database and click **Properties**.
3. Click **Options**.
4. In the Compatibility Level drop-down list, change the compatibility level to *SQL Server 2012 (110)*.

## **General PAM SC Troubleshooting and Maintenance Procedures**

This topic describes general PAM SC troubleshooting and maintenance procedures.

## **How to Verify That Privileged Access Manager Is Correctly Installed on Windows**

Verify that Privileged Access Manager is correctly installed immediately after you install the product. The following process helps you verify that Privileged Access Manager is correctly installed.

If the installation is successful, you see the following changes:

- A new key is added to the Windows registry:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl
```

While Privileged Access Manager is running, the keys and subkeys are protected. You can modify the keys only through Privileged Access Manager Endpoint Management or with `selang` commands. However, you do not need to use Endpoint Management or `selang` commands to read the keys and values.

- When you restart your computer, several new Privileged Access Manager services start automatically. These services include the Watchdog, Engine, and Agent, which are always installed. Other services, such as Task Delegation, exist depending on the options you chose during installation. The Display name for all Privileged Access Manager services begins with "." You can check what services are installed, and can verify that these services are running, using Windows Services Manager.

## **How to Troubleshoot Resource Access Problems**

Incorrect access authorities are the most common cause of resource access problems. An example of a resource access problem is a root user that can still access a protected resource, but the protected resource has a default access authority of none. The following process helps you troubleshoot resource access problems:

1. Change the audit mode for the protected resource to audit all:

```
chres CLASS ResourceName audit(all)
```

Changing the audit mode to audit all makes the audit log easier to read.

2. [Run a trace](#) and recreate the problem.
3. Review the trace file and the audit log for occurrences of the protected resource. Try to troubleshoot the cause of the resource access problem from the information in the files.

### **NOTE**

SPECIALPGM objects provide bypasses that are not audited, but these bypasses appear in the trace file.

**Note:** For assistance, contact Broadcom Support at <http://ca.com/support>.

## **How to Troubleshoot Connection Problems**

Many factors affect connections between Privileged Access Manager computers. Connection problems include being unable to connect to a remote computer, or the connection to the remote computer timing out. The following process helps you identify the cause of the connection problem.

**Note:** For assistance, contact Broadcom Support at <http://ca.com/support>.

1. Check the Privileged Access Manager computers for recent changes to the following items:
  - Encryption key
  - Encryption method
  - TCP and UDP ports
2. Review any new rules or recently changed rules in the following classes: TCP, CONNECT, HOSTNET, or HOST.
3. Determine the port that has the connection problem.
4. [Run a trace](#) and review the trace file for:
  - Connections that Privileged Access Manager blocked due to TCP rules or other rules
  - A code other than P (permitted) next to the port number that has the connection problem
5. Review the Privileged Access Manager audit log for D (deny) records that refer to the problematic port.
6. Check that firewalls do not block the problematic port.

7. Review the log files for your OS for error messages that are caused by ports that cannot bind.

### **How to Troubleshoot Performance Problems**

The following process helps you identify the cause of performance problems:

**Note:** For assistance, contact Broadcom Support at <http://ca.com/support>.

1. Identify when the performance problem occurs. Does performance degrade:
  - When the OS starts?
  - When Privileged Access Manager starts?
  - When Privileged Access Manager has been running for some time?
  - When Privileged Access Manager or the OS run a scheduled process?
  - (UNIX) When the Privileged Access Manager kernel extension is loaded?
  - When Privileged Access Manager daemons or services are loaded?
2. If you have determined that Privileged Access Manager causes the performance problem, investigate the following questions:
  - What processes are using the most resources when performance degrades?
  - Are the Privileged Access Manager processes keeping the same process ID throughout their lifecycle?
  - Are there any third-party filter drivers installed on the computer?
  - Are there any system-monitoring applications installed on the computer?
3. Check the Privileged Access Manager database:
  - a. Stop the product.
  - b. Check the database:
 

```
dbmgr -util -all
```
  - c. [Reindex the database](#).
  - d. [Rebuild the database](#).
  - e. Restart Privileged Access Manager and check if the problem still exists.
4. (Windows) Disable driver interception:
  - a. Stop Privileged Access Manager.
  - b. Change the value of the UseFsiDrv registry entry to 0. The UseFsiDrv registry entry is in the following registry key:
 

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl
```
  - c. Restart Privileged Access Manager and check if the problem still exists.
5. [Run a trace](#) and recreate the problem. Review the trace file for the following conditions:
  - Repeated events in a small period; for example, many file accesses in several seconds
  - Processes that have been killed
  - Either of the following values:
    - a. ACEEH = -1
    - b. U = a negative value
 These values can specify that Privileged Access Manager cannot resolve a user name or cannot assign a value to a resource.

### **NOTE**

For more information about improving Privileged Access Manager performance on your UNIX computer, see the Endpoint Administration Guide for UNIX.

### **Run a Trace**

Running a trace can help you troubleshoot problems. Privileged Access Manager writes trace records to the `seos.trace` file, which is located in the `ACInstallDir/log` directory.

**To run a trace:**

1. Remove all records from the trace file:

```
secons -tc
```

2. Start the trace:

```
secons -t+
```

3. Recreate the problem.

4. Stop the trace:

```
secons -t-
```

5. Review the trace file.

**NOTE**

The configuration settings in the seosd section configure the trace file. For more information about the seosd section, see the *Reference Guide*.

**Run a Trace on Privileged Access Manager Web Service Components****Valid on Windows**

Running a trace on the Privileged Access Manager web service components can help you troubleshoot problems. For example, if Privileged Access Manager Enterprise Management cannot connect to the DMS, run a trace to review the messages that these two components exchange.

Privileged Access Manager writes trace records for web service components to the file that is defined in the logFileName configuration setting in the WebService section. The default value for this configuration setting is C:\Program Files\CA\PAMSCServer\WebService\log\WebService.log.

**To run a trace on Privileged Access Manager web service components:**

1. Stop Privileged Access Manager and the Privileged Access Manager web service.

2. Create a registry key in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService\TraceEnabled
```

3. Set the value of the key to 1.

4. Start Privileged Access Manager and the Privileged Access Manager Web Service.

Tracing starts on the web service components.

5. Recreate the problem.

6. Stop Privileged Access Manager and the Privileged Access Manager web service.

Tracing stops on the web service components.

7. Set the value of the key to 0.

8. Review the trace file.

**Reindex the Privileged Access Manager Database**

Because many updates are made to the Privileged Access Manager database, the database files can become fragmented. Reindexing and [rebuilding the database](#) ensures database optimization for speed and reliability. Reindex the database during your routine maintenance procedures every three to six months, and whenever you have a performance problem.

**NOTE**

In this procedure, the Privileged Access Manager database is installed in the default location, /opt/CA/PAMSC/seosdb (UNIX) and C:\Program Files\CA\PAMSC\Data\seosdb (Windows). To perform this procedure, you must log in as a root user (UNIX) or as an administrator (Windows).



### To reindex the Privileged Access Manager database

1. Stop Privileged Access Manager.
2. Navigate to the following directory:
  - (UNIX) /opt/CA/PAMSC/seosdb
  - (Windows) C:\Program Files\CA\PAMSC\Data\seosdb

3. Back up the database:

```
dbmgr -backup backup_directory
```

4. Index the database:

```
dbmgr -util -build seos_cdf.dat
```

```
dbmgr -util -build seos_odf.dat
```

```
dbmgr -util -build seos_pdf.dat
```

```
dbmgr -util -build seos_pvf.dat
```

#### NOTE

To reduce the size of the database on UNIX computers further, use the `sepurgdb` utility to delete references to undefined records from the database. For more information about the `sepurgdb` utility, see the *Reference Guide*.

### Rebuild the Privileged Access Manager Database

Because many updates are made to the Privileged Access Manager database, the database files become fragmented. [Reindexing](#) and rebuilding the database ensures database optimization for speed and reliability. Rebuild the database during your routine maintenance procedures every three to six months.

#### NOTE

In this procedure, the Privileged Access Manager database is installed in the default location, /opt/CA/PAMSC/seosdb (UNIX) and C:\Program Files\CA\PAMSC\Data\seosdb (Windows). To perform this procedure, you must log in as a root user (UNIX) or as an administrator (Windows).

### To rebuild the Privileged Access Manager database:

1. Stop Privileged Access Manager.
2. Navigate to the following directory:
  - (UNIX) /opt/CA/PAMSC/seosdb
  - (Windows) C:\Program Files\CA\PAMSC\Data\seosdb

3. Back up the database:

```
dbmgr -backup backup_directory
```

4. Export the existing rules and the user-related data from the database:

```
dbmgr -export -l -f exported_filename
```

```
dbmgr -migrate -r migrated_filename
```

5. Navigate to the following directory and create a directory in it named `seosdb_new`:

- (UNIX) /opt/CA/PAMSC
- (Windows) C:\Program Files\CA\PAMSC\Data

6. Create a database in the `seosdb_new` directory using the following command:

```
dbmgr -create -cq
```

7. Copy the *exported\_filename* and *migrated\_filename* files to the `seosdb_new` directory.

8. Import into the new database the existing rules and user-related data that you exported from the old database:

```
selang -l -d "absolute path for seosdb_new" -f exported_filename
```

```
dbmgr -migrate -w migrated_filename
```

**NOTE**

Selang does not use -d option. If you run the "selang -l -f exported\_filename" command after stopping the Privileged Access Manager service and move to the seosdb\_new directory, the exported rules are stored in \$SEOSDIR/seosd.

9. Rename the seosdb directory to seosdb\_old.
10. Rename the seosdb\_new directory to seosdb.
11. Start Privileged Access Manager.

**Change Port Number for Privileged Access Manager Agent Communication**

Privileged Access Manager client applications such as selang, policydeploy, and devcalc, and the Privileged Access Manager Agent communicate on port 8891. We do not recommend that you change this port. If you do change this port, use the following procedure.

**To change the port number for Privileged Access Manager Agent Communication:**

1. Open the following file in a text editor:
  - (UNIX) /etc/services
  - (Windows) %SystemRoot%\drivers\etc\services
2. Add the following file to the file:
 

```
seoslang2 port-number/ tcp
```
3. Save and close the file.
4. Restart Privileged Access Manager daemons or services.

**Configure the Message Queue TCP Port**

When you install Privileged Access Manager Enterprise Management, by default you configure the Message Queue to work with the SSL port. You can change this default behavior and can configure the Message Queue to use the TCP port.

**To connect to the Message Queue TCP port:**

1. Stop the WildFly Server, the Endpoint Services (secons -s), and the Privileged Access Manager ActiveMQ Broker.
2. Open the file C:\ActiveMQ\conf\activemq.xml for editing.

Replace this line of code:

```
<transportConnector name="nio+ssl" uri="nio+ssl://0.0.0.0:61616?
maximumConnections=1000&needClientAuth=false&transport.enabledProtocols=TLSv1.2&w
>
```

With this line of code:

```
<transportConnector name="nio" uri="nio://0.0.0.0:61615?
maximumConnections=1000&needClientAuth=false&wireFormat.maxFrameSize=104857600" /
>
```

3. Save the file and close the file.
4. Open the file standalone-full.xml for editing. The file is in the following location:

```
<WildFly_Home>\standalone\configuration
```

Replace the two instances of the following line of code:

```
ssl://localhost:61616?socket.enabledProtocols=TLSv1.1,TLSv1.2
```

With the following line of code:

```
tcp://localhost:61615
```

5. Save the file and close the file.
6. Open the registry editor. Edit the value in the following key:

```
HKEY_LOCAL_MACHINE>SOFTWARE>ComputerAssociates>AccessControl>Common>communications>Distribution_Server
Replace
```

```
ssl://localhost:61616
```

```
with
```

```
tcp://localhost:61615
```

7. Start the CA Privileged Identity Manager ActiveMQ Broker, Endpoint Services (seosd -start), and .WildFly

### **Information to Provide to Broadcom Support**

When you contact Broadcom Support, they will ask you to provide information about any changes to the environment to help them diagnose the cause of the problem. For example, host and user name changes and changes to the operating system can affect Privileged Access Manager. Broadcom Support might also ask you to use the Privileged Access Manager Support utility to provide more diagnostic information.

Broadcom Support asks you to provide the following information:

- Privileged Access Manager version
- Operating system name, version, architecture, and update level
- Details of any Privileged Access Manager patches installed on the computer
- Number of CPUs

#### **NOTE**

For more information about the operating systems, versions, architectures, and update levels that Privileged Access Manager supports, see the Compatibility Matrix that is available from the Privileged Access Manager product page on [Broadcom Support](#).

Broadcom Support might ask you the following questions:

- What is the impact of the problem?
- When did the problem first occur?
- Is the problem reproducible?
- Was anything added, removed, or changed in the environment before the problem occurred?
- Did you restart the computer before the problem occurred?
- How many times has the problem occurred?
- What happens on the system when the problem occurs? For example, does the problem occur when you execute a particular process or command?
- Does the problem occur consistently or randomly?
- Do any segmentation faults or access violations occur when you execute a Privileged Access Manager command?
- Why do you think Privileged Access Manager caused the problem?
- If the problem is an operating system problem, did you report the problem to the operating system vendor? If yes, can you provide a crash analysis from the operating system vendor?

### ***Generate Diagnostic Information About a Windows Endpoint***

When a customer contacts Broadcom Support to report a Windows endpoint issue, the support team often asks for customer environment information to help diagnose the issue. Privileged Access Manager provides a standalone utility that helps a customer collect relevant information (for example, the Event log, Dump files, System information) from an endpoint. The customer provides the output that the utility generates to the Broadcom Support so that they can troubleshoot the issue. The script is included in the customer endpoint implementation.

The utility lets you collect and report the following information about a Windows endpoint to Broadcom Support:

- System Information
- Export Event log
- Common Information
- Export Privileged Access Manager Registry
- Export Privileged Access Manager Audit
- Copy Privileged Access Manager Audit
- Export Privileged Access Manager Database
- Copy Privileged Access Manager Trace
- Copy Configuration Files
- List Privileged Access Manager Files
- Get Authentication and Cache Statistics
- Export APM Database
- Copy Dump Files
- Export Policy Management Database
- Export Policy Management Database Audit
- Copy Policy Management Database Audit
- Export APM Audit
- Copy APM Audit
- Copy Instrumentation Trace
- Copy APM Logs
- Copy Database

If you collect a copy of the Privileged Access Manager database, the Support utility stops the product before it takes a snapshot of the database. The Support utility restarts Privileged Access Manager when the snapshot is complete.

You can run the support utility in any of the following modes:

- **Interactive Mode**

Follow these steps to run the Support utility in the Interactive mode:

- a. Navigate to the directory where you have installed Privileged Access Manager endpoint: `ACInstallDir\bin`
- b. Double-click **ACSupport.exe**.
- c. In the **ACSupport** dialog that appears, select report types that you want the Support utility to collect and click **Proceed**.

The Support utility takes a snapshot and places the output in the `ACInstallDir\ACSupport` directory.

- **Silent Mode**

Follow these steps to run the Support utility in the Silent mode:

- a. Open a command prompt.
- b. Run the following command:

`ACSupport -s`

If you run the utility without a parameter, the utility starts in the interactive mode.

When you run this command, the utility collects information from a Windows endpoint based on the configuration tokens set in the **CFG\_support.ini** file. The configuration file is created during the endpoint installation, and placed in the Data directory of the installation path. By default, all the configuration tokens are set to "yes." Set the configuration token to "No" in case you do not want the utility to collect any information. The Support utility takes a snapshot and places the output in the `ACInstallDir\ACSupport` directory.

You find one-one correspondence between the Report types available from the **ACSupport** dialog and the tokens in the **CFG\_support.ini** file. Also, the meaning of each token is intuitive in the **CFG\_support.ini** file.

### **Generate Diagnostic Information About a UNIX Endpoint**

The Privileged Access Manager Support utility collects information about your installation to help Broadcom Support diagnose the cause of problems. If you include the Privileged Access Manager database in the snapshot, the Support

utility stops the product before it snapshots the database. The Support utility restarts Privileged Access Manager when the snapshot is complete.

The Privileged Access Manager Support utility always collects the following information about UNIX endpoints:

- `seos.ini` The Privileged Access Manager initialization file
- `tmpetc` The files from the Privileged Access Manager `/etc` directory, including the following:
  - `audit.cfg` The audit filter file
  - `auditroute.cfg` The audit route filter file
  - `nfsdevs.init` A file that contains the NFS defaults for the major device numbers for each operating system
  - `osver` The operating system version
  - `sereport.cfg` The sereport configuration file
  - `serevu.cfg` The serevu configuration file
  - `trcfilter.init` The trace filter file
- `versions.txt` A file that contains versions of key Privileged Access Manager binaries
- Some operating system files, for example, some variable files

If you specify that the Privileged Access Manager Support utility collects information about the database, it collects the following information:

- `seosdb` The Privileged Access Manager database
- `seosdb.tar` A compressed file of the Privileged Access Manager database
- The lookaside databases for groups, hosts, services, and users

If you specify that the Privileged Access Manager Support utility collects information about the logs, it collects the following information:

- `tmplog` The Privileged Access Manager log files
- `log.tar` A compressed file of the Privileged Access Manager log directory

### To generate diagnostic information about a UNIX endpoint

1. Navigate to the following directory, where *ACInstallDir* is the directory in which you installed Privileged Access Manager:

```
ACInstallDir/lbin
```

2. Execute the following command:

```
./support.sh [-db] [-log] [-all] [-none]
```

- **-db**  
Collects information about `seosdb`, the Privileged Access Manager database, but does not collect information about the audit logs.
- **-log**  
Collects information about the audit logs but does not collect information about `seosdb`.
- **-all**  
Collects information about both `seosdb` and the audit logs.
- **-none**  
Does not collect information about `seosdb` and the audit logs.

#### NOTE

If you do not specify an option, the Privileged Access Manager Support utility runs in interactive mode.

The Privileged Access Manager Support utility snapshots your installation and places the output in the *ACInstallDir* directory.

### Generate Diagnostic Information About The Enterprise Management Server

When a customer contacts Broadcom Support to report an Enterprise Management Server issue, the support team often asks for customer environment information to help diagnose the issue. Privileged Access Manager provides a Log Collector script that helps a customer collect relevant information (for example, the WildFly server log, installation logs) from the Enterprise Management Server. The customer provides the output that the script generates to the Broadcom Support so that they can troubleshoot the issue. The script is included in the customer Enterprise Management Server implementation.

Follow these steps to run the log collector script file:

#### [Windows]

1. Open a command prompt.
2. Navigate to *ACInstallDir\PAMSCServer\IAM Suite\Access Control\tools\LogCollector*.
3. Run the *log.bat* file.  
The script runs and collects the support information in a compressed file (ENTM\_supportfile\_<Date>.zip). The compressed file is placed in the **LogCollector** directory.

#### [Linux]

1. Open a terminal session.
2. Navigate to *ACInstallDir/PAMSC/Server/IAM Suite/Access Control/tools/LogCollector*.
3. Run the *log.sh* file.  
The script file runs and collects the support information in a compressed file (ENTM\_supportfile\_<Date>.zip). The compressed file is placed in the **LogCollector** directory.

## Install PAM Server Control Endpoints and Server Components

### Required packages are Missing for Linux Installation

#### Symptom:

The installation fails because required Linux packages are missing.

#### Solution:

Use the `rpm --requires` and the `rpm --which` provides commands to verify package dependencies, and install missing packages.

**Note:** For more information about required packages, see Required 32-bit Packages for installing the Enterprise Management Server on Red Hat Linux 6, in the Installation Considerations section of the *Privileged Access Manager Release Notes*.

#### ***rpm --requires Detect Library Dependencies***

When installing Enterprise Management on Linux, you want to know on which libraries the CAeAC package depends.

The command uses the following syntax:

```
rpm -qp --requires package
```

The command has the following parameters:

- **-q**  
Specifies that you want to query RPM package information.
- **-p**  
Query an RPM package file. Also retrieves information about packages that are not installed.
- **--requires package**

Retrieves the dependencies that are required by the package.

### Example

You want to retrieve dependency information about Privileged Access Manager 12.8 SP0.

```
root> rpm -qp --requires CAeAC-1280-0.0.1275.i386.rpm

rpm >= 4.0

libcrypt.so.1

libc.so.6

libdl.so.2

libgcc_s.so.1

libm.so.6

libnsl.so.1

libpam.so.0

libpthread.so.0

libresolv.so.2

libstdc++.so.6

rpmLib(PayloadFilesHavePrefix) <= 4.0-1

rpmLib(CompressedFileNames) <= 3.0.4-1
```

Continue running the rpm command on the listed packages one by one to retrieve further dependencies.

```
root> rpm -qp --requires libcrypt
```

### ***rpm --whatprovides Verify That a Library Exists***

Before installing Enterprise Management on Linux, verify that all required libraries are present on the target system.

The command uses the following syntax:

```
rpm -q --whatprovides capability
```

The command has the following parameters:

- **-q**

Specifies that you want to query RPM package information.

- `--whatprovides capability`

Specifies that you want to retrieve information which packages provide the capability.

### Example: Verify that a library is installed

In this example, you want to verify that `libcrypt.so.1` is installed. You receive a positive answer (`$?` is 0) and you learn that it is the `glibc-2.5-42` package that provides `libcrypt.so.1`.

```
root> rpm -q --whatprovides libcrypt.so.1

glibc-2.5-42

root> echo $?

0
```

### Example: Detect that a library is not installed

In this example, you want to find out whether `libexample.so.1` is installed. You receive a negative answer (`$?` is 1), because no package is installed that provides this capability.

```
root> rpm -q --whatprovides libexample.so.1

no package provides libexample.so.1

root> echo $?

1
```

If a required library is missing, install it before proceeding the installation.

## Modify the Oracle Database Host Settings After Installation

### Symptom:

After installing the Enterprise Management Server, I need to modify the Oracle database server settings to point to a different server.

### Solution:

You can modify the Enterprise Management Server to work with an Oracle database on a different host after installation:

1. Stop the WildFly service on the Enterprise Management Server.
2. Back up the Oracle database on the current host.
3. Restore the Oracle database on the new host.
4. Navigate to the following directory, where *WildFly\_HOME* indicates the directory where you installed WildFly:

```
WildFly_HOME/standalone/configuration
```

5. Locate and back up the following file:
  - `standalone-full.xml`



6. Open the file and locate the <connection-url> entry.
7. Modify the connection settings to specify the new Oracle database host name except the pool name **ExampleDS**.

**Example:**

```
<connection-url>jdbc:oracle:thin@//new_host_name:1521/sid_or_service_name</
connection-url>
```

8. Start the WildFly service.  
You have modified the Oracle database host settings.

**Enterprise Management Server Fails To Register Endpoints Type****Symptom:**

I cannot view the endpoint types when I attempt to register the endpoint, after installing the Enterprise Management Server.

**Solution:**

The componentregistration utility registers the endpoints with the Enterprise Management Server. When the installation fails to register the endpoints, you can manually run the componentregistration utility.

**Follow these steps:**

1. Log in to the Enterprise Management Server.
2. Open a Command Prompt window and navigate to the following bin directory:

```
\ProgramFiles\CA\PAMSCServer\APMS\PAMSC\bin\
```

3. Run the following command to execute the ComponentRegistration utility:

```
ComponentRegistration -comp jcs -register -userDN <user> -serverDN <server> -pwd
<communication_password> -port CA Portal -ssl yes
```

For example: ComponentRegistration -compjcs -register -userDNcn=root,dc=etasa -serverDN dc=im,dc=etasa -pwdpassword-port 20411 -ssl yes

4. Restart Privileged Access Manager Services.
5. Verify that the endpoint types are registered by logging in to Privileged Access Manager Enterprise Management.
6. Browse to Privileged Accounts, Endpoints, View Endpoints Types and check the listed endpoints types.

You have successfully registered the endpoint types.

**"Bad Interpreter" Error Message During CA Privileged Access Manager Server Control Enterprise Management Installation****Valid on UNIX and Linux****Symptom:**

When I try to install Privileged Access Manager Enterprise Management, I receive the following error message:

```
/bin/sh: bad interpreter: Permission denied
```

**Solution:**

In some UNIX or Linux releases, the operating system automounts the optical disc drive with the noexec option. To install Privileged Access Manager Enterprise Management, verify that the optical disc drive is not mounted with the noexec option.

### **Cannot Use '\$' Character for CA Privileged Access Manager Server Control Enterprise Management Database Password**

#### **Symptom:**

When I install Privileged Access Manager Enterprise Management, I enter the database password and I receive the following error message: "Database version could not be detected".

#### **Solution:**

Privileged Access Manager Enterprise Management installation displays this error message if you enter a '\$' character at the end of the password. If you must place a '\$' character at the end of the password, you must change the database password after the installation.

### **Cannot Open CA Privileged Access Manager Server Control Server Components**

#### **Symptom:**

I cannot open Privileged Access Manager Enterprise Management, Endpoint Management, or Password Manager in a web browser after I start all prerequisite services. I have installed WildFly and Oracle on the same server.

#### **Solution:**

Both Oracle and WildFly use a default port of 8080. To fix this problem, you must resolve the port conflict between Oracle and WildFly. You should consider which change is easiest to implement in your enterprise before you change the Oracle or WildFly port.

Use the following procedures to change the default WildFly and Oracle ports:

#### **Follow these steps:**

1. Stop WildFly.
2. Open the following file in a text editor:  
`<WildFly_Home>/standalone/configuration/standalone-full.xml`
3. Change the port number in the following section:  
`<socket-binding name="http" port="8080"/>`
4. Save and close the file.
5. Start WildFly.
6. (Windows) Change the Privileged Access Manager Enterprise Management, Endpoint Management, and Password Manager shortcuts, as follows:
  - a. Click Start, Programs, CA, Access Control, and right-click the appropriate shortcut.  
 For example, to change the Privileged Access Manager Enterprise Management shortcut, click Start, Programs, CA, Access Control, and right-click Enterprise Management.
  - b. Click Properties.
  - c. Change the port number in the URL field to the new WildFly port number.

#### **To change the default Oracle port:**

1. Start the SQL command line.
2. Connect to Oracle as sysdba:

```
connect / as sysdba
```

3. Check what port is currently used for HTTP communication:

```
select dbms_xdb.gethttpport from dual;
```

4. Set the port to the desired port number:

```
exec dbms_xdb.sethttpport('portNumber');
```

5. Stop and restart the database.

```
shutdown immediate
```

```
startup
```

## **No Tabs Visible in CA Privileged Access Manager Server Control Enterprise Management**

### **Valid for Active Directory user stores**

#### **Symptom:**

I successfully install Privileged Access Manager Enterprise Management. When I log in as the system user that I specified during installation, no tabs appear in the interface.

#### **Solution:**

When you install Privileged Access Manager Enterprise Management, you provide the following Active Directory parameters:

- Host
- Port
- Search root
- User DN (and the password for this user)
- System User

This problem occurs when the Active Directory search root is in the same node in the directory tree as the DNs (Distinguished Names) for User DN and System User. To fix this problem, specify a search root one or more nodes higher in the directory tree than the DNs for the specified User DN and System User.

#### **Example: The Active Directory Search Root**

This example uses the following DNs for User DN and System User:

- User DN: CN=MyQueryUser,OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
- System User: CN=MySystemManager,OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB

The following search root is one node higher in the directory tree than the DNs for User DN and System User. If you specify the following search root, Privileged Access Manager Enterprise Management successfully installs and tabs appear in the interface:

```
OU=NFS, OU=ACCOUNTS, DC=EXAMPLE, DC=LAB
```

The following search root is in the same node in the directory tree as the DNs for User DN and System User. If you specify the following search root, Privileged Access Manager Enterprise Management successfully installs but no tabs appear in the interface:

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

### Example: Set the Active Directory Search Root One Node Higher In the Directory Tree

This example uses the same DNs for User DN and System User as the previous example.

In this example, you specified the following search root when you installed Privileged Access Manager Enterprise Management:

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

Because this search root is in the same node in the directory tree as the DNs for User DN and System User, specify a search root one node higher in the directory tree.

#### To set the Active Directory search root one node higher in the directory tree:

1. Enable the CA Identity Manager Management Console.
2. Open the CA Identity Manager Management Console.
3. Click Directories, and click the ac-dir directory.  
The Directory Properties dialog appears.
4. Click Export at the bottom of the Directory Properties dialog.
5. When prompted, save the XML file and open it for editing.  
**Note:** The file name is ac-dir.xml.
6. Locate the tag that contains the search root that you specified during installation. For example:

```
<LDAP searchroot="OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
```

7. Replace the existing search root with the new search root. For example:

```
<LDAP searchroot="OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
```

**Note:** Because you removed the Enterprise OU (Organizational Unit), this search root is one node higher in the directory tree than the previous search root.

8. Save and close the file.
9. In the CA Identity Manager Management Console, click Update in the Directory Properties dialog.  
The Update Directory page appears.
10. Click Choose File, navigate to the XML file that you edited, click Open, and click Finish.  
The CA Identity Manager Management Console validates the XML file and displays status information in the Directory Configuration Output field.  
**Note:** If you receive a "Failed to Import" error, see the Cannot Import ac-dir.xml Directory Configuration File topic.
11. Click Continue.  
The Directories page appears.
12. Click ac-dir, and click ac-env in the Environment(s) section.  
The Environment Properties page appears.
13. Click Restart.  
The CA Identity Manager Management Console restarts the environment and applies your changes.

**Note:** For more information about how to enable and start the CA Identity Manager Management Console, see the *Implementation* section.

## **Cannot Import ac-dir.xml Directory Configuration File**

### **Symptom:**

I exported the ac-dir.xml directory configuration file from the CA Identity Manager Management Console. When I try to import the file, the following error message appears in the Directory Configuration Output field:

```
Deploying directory configuration...
```

```
Parsing input stream...
```

```
Error: (140:67): cvc-complex-type.4: Attribute "value" must appear on element
"Container".
```

```
Error: Failed to import
```

```
*****
```

```
1 error(s), 0 warning(s)
```

### **Solution:**

The ac-dir.xml directory configuration file describes the structure and content of the user store. You use this file to change how Privileged Access Manager Enterprise Management interacts with the user store, for example, to change the user directory password or the Active Directory search root. You also edit the ac-dir.xml file when you configure Privileged Access Manager Enterprise Management for SSL communication and Active Directory for failover.

To fix this problem, do the following:

1. Open the ac-dir.xml file for editing.
2. Locate the following tag:

```
<Container objectclass="top,organizationalUnit" attribute="ou"/>
```

3. Replace the previous tag with the following tag:

```
<Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
```

4. Save and close the file.

You can now import the directory configuration file in to the CA Identity Manager Management Console. To apply any changes that you made in the directory configuration file, you must restart the environment after you import the file.

## **CA Privileged Access Manager Server Control Enterprise Management Cannot Connect to DMS**

### **Symptom:**

When I log in to Privileged Access Manager Enterprise Management, I receive a message similar to the following:

```
Error: Login procedure failed
```

```
Error: Password on target does not match client's password
```

### **Solution:**

The user `ac_entm_pers` cannot log in to the DMS. This user authenticates communication and data flow between the Enterprise Management Server and the DMS.

**Note:** The `ac_entm_pers` user has the following authorization attributes: ADMIN, AUDITOR, IGN\_HOL, LOGICAL

To troubleshoot this problem, do the following:

1. Open `selang`.
2. Connect to the DMS:

```
host DMS__@entM_host_name
```

3. Change the password for `ac_entm_pers`:

```
eu ac_entm_pers admin auditor nonative password(password) logical nonative grace-
```

4. Authorize `ac_entm_pers` to log in to the host on which the Enterprise Management Server is installed:

```
authorize TERMINAL entM_host_name uid(ac_entm_pers) access(a)
```

5. Validate that `ac_entm_pers` can log in to the Enterprise Management Server:

```
host DMS_@entM_host_name uid(ac_entm_pers) password(password) logical
```

6. Update the Enterprise Management Server DMS connection settings with the new password for `ac_entm_pers`. The DMS authenticates `ac_entm_pers` and Privileged Access Manager Enterprise Management is connected to the DMS.

**Note:** For more information about how to configure the connection to the DMS, see the *Privileged Access Manager Enterprise Management Online Help*.

If you receive an error when you update the connection settings, the DMS cannot authenticate `ac_entm_pers`. To troubleshoot this problem, do the following:

1. Verify that you entered the same password in each step of the previous procedure.
2. Verify that the host name of the Enterprise Management Server (*entM\_host\_name*) in Step 4 of the previous procedure is correct.  
For example, if you specify the fully qualified host name of the Enterprise Management Server in Step 4, but the `TERMINAL` record for the Enterprise Management Server uses a short host name, the host names are not resolved. `ac_entm_pers` cannot log in to the Enterprise Management Server.
3. Review the Privileged Access Manager audit file:

```
seaudit -a
```

#### 4. Review the DMS audit file:

```
seaudit -a -fn DMS_log_file
```

**Note:** The audit records may provide information about the correct host name of the TERMINAL record for the Enterprise Management Server.

#### **Example: Display the DMS Audit File**

The following example displays the audit file for a DMS named DMS\_\_:

```
seaudit -a -fn "C:\Program Files\CA\PAMSCServer\APMS\PAMSC\Data\DMS__\pmd.audit"
```

### **Question Marks Appear in CA Privileged Access Manager Server Control Enterprise Management Tabs**

#### **Symptom:**

When I open Privileged Access Manager Enterprise Management, I see question marks in the tabs.

#### **Solution:**

To fix this problem, change the default language of your browser to US English.

### **Received "Null page" Error in InfoView**

#### **Symptom:**

When I try to access the Privileged Access Manager reports I get the following error in InfoView:

```
Null page: Unable to create page from report source
```

#### **Solution:**

On Windows, the Privileged Access Manager Universe may not be defined or installed properly. Test the connection for the Privileged Access Manager Universe. If the connection is not working, edit the connection; if the connection is working, replace the connection.

On Solaris, log in as bouser and edit the script \$CASHCOMP/CommonReporting/bobje/setup/env.sh as follows:

#### 1. Append the following LIBRARYPATH:

```
$MWHOME/lib-sunos5_optimized
```

#### 2. Restart BusinessObjects services:

```
cd $CASHCOMP/CommonReporting/bobje
```

```
./stopservers
```

```
./startservers
```

## **CA Privileged Access Manager Server Control Does Not Start Automatically After a UNIX Installation**

### **Valid on UNIX**

#### **Symptom:**

Privileged Access Manager does not start automatically after I install it on a UNIX endpoint.

#### **Solution:**

By default, Privileged Access Manager does not start automatically on a UNIX endpoint.

To configure the seosd daemon to start automatically upon startup on a UNIX computer, use the *ACInstallDir/samples/system.init/sub-dir* directory, where *sub-dir* is the directory for your operating system. Each sub-directory contains a readme file with instructions on how to start Privileged Access Manager automatically on your operating system.

**Note:** For more information about how to start Privileged Access Manager, see the *Implementation* section.

## **Cannot Start Daemons on Linux s390 Endpoint**

### **Valid on Linux s390 and Linux s390x**

#### **Symptom:**

I cannot start the seosd or ReportAgent daemon.

#### **Solution:**

Privileged Access Manager cannot locate the Java environment on the endpoint. To fix this problem, do the following:

1. Verify that the `java_home` configuration setting in the global section of the `accommon.ini` file contains the path to the Java environment.
2. Set the value of the `LD_LIBRARY_PATH` environment variable to the path to the shared libraries of the Java environment.

## **Cannot Connect to selang After Installation**

#### **Symptom:**

After I install Privileged Access Manager, I receive the following error when I try to start selang or connect to the Privileged Access Manager database:

```
ERROR: Initialization failed, EXITING!
```

```
(localhost)
```

```
ERROR: Login procedure failed
```

```
ERROR: You are not allowed to administer this site from terminal example.com
```

#### **Solution:**

Terminal rules are not correctly defined. Troubleshoot the terminal rules to determine the problem.

#### **To troubleshoot terminal rules:**

1. Stop Privileged Access Manager:

```
secons -s
```



2. Start `selang` in local mode:

```
selang -l
```

**Note:** You must be the root user to run `selang` in local mode on a UNIX computer.

3. Check that you have created a `TERMINAL` record for the local terminal (*terminal\_name*), and that the terminal access authorities are correctly defined:

```
showres TERMINAL terminal_name
```

- If a record does not exist, create a `TERMINAL` record for the local terminal:

```
editres TERMINAL terminal_name owner(name) defaccess(accessAuthority)
```

**Note:** The owner can be either a user or a group. Because the default access for a `TERMINAL` record is none, we recommend that you specify a default access when you create the record to avoid locking users out of the terminal.

- If the terminal access authorities are incorrect, define the correct access authorities for the terminal:

```
authorize TERMINAL terminal_name uid(name) access(accessType)
```

4. (UNIX) Check the value of the `terminal_default_ignore` configuration setting in the `[seosd]` section. This configuration setting determines if Privileged Access Manager considers the `defaccess` value of the `_default` `TERMINAL` and of the specific `TERMINAL` records when authorizing administrative access.

**Note:** For more information about the `terminal_default_ignore` configuration setting, see the *Reference* section.

5. (UNIX) Check that the lookaside database reflects the terminal, as follows:

- a. Build a hostname-specific lookaside database:

```
sebuilda -h
```

- b. Check that the terminal entry and the hostname are the same in the lookaside database:

```
sebuilda -H | grep hostname
```

The contents of the hosts lookaside database files are listed.

6. Start Privileged Access Manager:

- (UNIX) `seload`
- (Windows) `seosd -start`

**Note:** If you still cannot start `selang` or connect to the Privileged Access Manager database, you may have to modify the hosts file for your OS. Contact your system or network administrator for assistance.

### **Messages Appear in Solaris 10 Log File**

#### **Valid on Solaris 10**

#### **Symptom:**

When I stop Privileged Access Manager using "`secons -s`," messages appear in the `/var/adm/messages` log file on my Solaris 10 computer. The `SEOS_use_streams` configuration setting on my computer is set to yes.

**Solution:**

These messages are informational only and do not indicate any failure or error. You do not need to do anything. The messages and their interpretation follow:

- "SEOS: Restored tcp wput" "SEOS: Restored strthead rput"  
These messages indicate that the SEOS\_syscall function disabled network hooks.
- "SEOS: Replaced tcp wput" "SEOS: Replaced strthead rput"  
These messages indicate that the SEOS\_syscall function enabled network hooks.

**Received Error When Manually Deleting Registry Keys During Uninstall****Valid on Windows****Symptom:**

When I try to delete a registry key while uninstalling Privileged Access Manager, I receive the following error message:

```
Cannot open Data: Error while opening key.
```

**Solution:**

Run the RemoveAC.exe utility to remove Privileged Access Manager registry keys and directories. The RemoveAC.exe utility does not uninstall the product, but helps ensure that all Privileged Access Manager registry keys and directories are removed from the computer.

**ProductExplorer Not Started****Symptom:**

When I insert the Privileged Access Manager Server Components DVD for Windows into my optical drive, the ProductExplorer does not start.

**Solution:**

Do the following:

- Navigate to the optical disc drive directory and double-click the ProductExplorerrx86.EXE file.
- Enable autorun to startup the ProductExplorer automatically.

**The Path/Environment Variable Is Not Set In a Solaris Endpoint****Symptom:**

When I do `sesu` to root in a Solaris endpoint from any non-root user, the path/environment variable for the root user is not set.

Sample Error Message:

```
bash-2.05$ sesu -
Sun Microsystems Inc. SunOS 5.9 Generic May 2002
You have new mail.
/etc/profile[121]: grep: not found
/etc/profile[121]: uname: not found
/etc/profile[121]: test: argument expected
/etc/profile[121]: uname: not found
```

```

/etc/profile[121]: uname: not found
/etc/profile[121]: test: argument expected
.profile[5]: grep: not found
.profile[5]: uname: not found
.profile[5]: test: argument expected
.profile[5]: uname: not found
.profile[5]: grep: not found
.profile[5]: uname: not found
.profile[5]: test: argument expected

```

**Solution:**

1. Stop Privileged Access Manager services.  

```
#/opt/CA/PAMSC/bin/secons -s
```
2. Open seos.ini file for editing. You can find this file at /opt/CA/PAMSC/.
3. Modify the following lines in seos.ini as follows, and save the file.

```

old_sesu = no
request_target_password = no
UseInvokerPassword = no

```

4. Start Privileged Access Manager services.

```
#/opt/CA/PAMSC/bin/seload
```

**Login Procedure Failed Error in a UNIX Endpoint****Symptom:**

After a successful installation of a UNIX endpoint, I get the following error on starting selang or when I connect to SEOSDB.

```

"ERROR: Initialization failed, EXITING!"(localhost)
ERROR: Login procedure failed
ERROR: You are not allowed to administer this site from terminal 127.0.0.1

```

**Solution:**

Verify that the terminal rules are defined properly. If not, define the proper terminal and provide appropriate authorization for the terminal.

1. Stop Privileged Access Manager endpoint services.

```
/opt/CA/PAMSC/bin/secons -sk
```

2. Start Selang in local mode.

```
selang -l
```

3. Verify if the terminal with the host name is defined and proper authorizations are provided.

```
PAMSC> sr terminal *
```

If not, define the terminal and provide the appropriate authorization.

```
PAMSC> authorize TERMINAL <terminal name> uid(USER) access(Type of access to be
provided)
```

4. Quit selang
5. Check if the Look Aside Database (LADB) reflects the defined host name terminal according to your site. Use `sebuildla -h` to build the host name-specific LADB.
6. Use `sebuildla -H | grep <hostname>`, to match against the defined terminal entry. The terminal entry and the host name must be same in all aspects.
7. Check if the TERMINAL class is ON. If it is OFF, run "so CLASS+(TERMINAL)" from the Selang prompt.
8. Start Privileged Access Manager services.

### **Ungraceful Shutdown of a Process Causes Corruption**

#### **Symptom:**

The SIGKILL signal is sent to a process to terminate (kill) it immediately. In contrast to SIGTERM and SIGINT, this signal cannot be caught or ignored, and the receiving process cannot perform any clean-up upon receiving this signal.

#### **Solution:**

To protect programs from being killed while Privileged Access Manager is up and running, define relevant PROCESS rules for the binaries. Try **secons -S selogrd** or **kill -15 PID**, which gives the components a chance to shut down correctly and safely (closing socket connections, cleaning up temp files, and informing the child processes that it is going away).

### **Error Starting SEOS**

#### **Symptom:**

When I start Privileged Access Manager services through seload on a Linux endpoint, I get the following error message:

```
./seload
CA Privileged Access Manager Server Control seload <version> - Loader Utility
Copyright (c) 2013 CA. All rights reserved.
SEOS_load: Warning ! The system.map file does not exist
on this system. As a result CA Privileged Access Manager Server Control might
not be able to load
SEOS_load: Executing un/load exit file, /opt/CA/PAMSC/exits/LOAD/SEOS_load_int.always -
pre
SEOS_load: Executing un/load exit file, /opt/CA/PAMSC/exits/LOAD/SEOS_load_int.always -
post
SEOS_load: SEOS_syscall WASN'T loaded
```

#### **Solution:**

Run the following command to check if the **system.map** file is available:

```
ls -al /boot/System.map-`uname -r`
```

If the file is missing, install it. This file is required to load/get debug information from the kernel module.

## **Failed to Unload Privileged Access Manager Endpoint**

### **Symptoms:**

When I uninstall Privileged Access Manager endpoint, I get the following error messages:

```
Trying to unload CA Privileged Access Manager Server Control...
```

```
ERROR: Module seos is in use
```

```
Error: CA Privileged Access Manager Server Control kernel module could not be unloaded.
```

### **Solutions:**

You can troubleshoot this problem using the following two ways:

#### **Solution 1**

1. Run the following command to list all the dependent processes (intercepted system calls) on SEOS kernel module.

```
secons -scl'
```

Example:

```
# secons -scl
CA Privileged Access Manager Server Control secons v12.81.0.2627 - Console utility
Copyright (c) 2015 CA. All rights reserved.
Active system calls:
-Syscall 2 - PID: 14412 PPID: 27271 UID: 0 TIME: 10s PROGRAM NAME: /bin/cat
```

2. Stop the listed dependent processes:

```
# Kill -15 <pid>
```

Example:

```
# kill -15 14412
```

3. Run the following command to stop and kill the endpoint daemons or services:

```
# secons -skca c
```

4. Unload the kernel module using the following command.

```
# SEOS_load -u
```

5. Uninstall the endpoint, if necessary.

```
# ./uninstall_AC
```

**Note:** If the uninstall fails, run the following command to uninstall the endpoint.

- # rpm -e CAeAC (for native package installation)
- # ./uninstall\_AC -force (for install\_base installation)

#### **Solution 2:**

1. Reboot the endpoint so that the dependent processes on the kernel module are cleared from the system.
2. Run the following command to stop and kill the endpoint daemons or services:

```
# secons -sk
```

3. Unload the kernel module using the following command.

```
# SEOS_load -u
```

4. Uninstall the endpoint, if necessary.

```
# ./uninstall_AC
```

**Note:** If the uninstall fails, run the following command to uninstall the endpoint.

- # rpm -e CAeAC (for native package installation)
- # ./uninstall\_AC -force (for install\_base installation)

### **ORA-00955: Name Is Used by an Existing Object**

#### **Symptom:**

When I restart WildFly, the following error is shown in the **server.log** file:

```
ERROR [ims.tmt.CreateDatabaseSchema] Error in creating Report Snapshot database schema.
java.sql.SQLException: ORA-00955: name is already used by an existing object
    at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:447)
    at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:396)
    at oracle.jdbc.driver.T4C8Oall.processError(T4C8Oall.java:951)
    at oracle.jdbc.driver.T4CTTIfun.receive(T4CTTIfun.java:513)
    at oracle.jdbc.driver.T4CTTIfun.doRPC(T4CTTIfun.java:227)
    at oracle.jdbc.driver.T4C8Oall.doOALL(T4C8Oall.java:531)
```

#### **Solution:**

When you install the Enterprise Management Server, all the tables are created in the database. Post installation when WildFly starts, it tries to create some tables again. Because the tables already exist in the database, you see errors in the **server.log** file. You can ignore this error as it has no impact on the product.

## **Create Policies and Access Authorities**

### **Block Users Access to Network Drives and Shared Drives**

#### **Valid on Windows**

#### **Symptom:**

I am able to block users access to a system drive, but I cannot stop users access to network and shared drives.

#### **Solution:**

To block users access to network and shared drives on Windows 2008, add the following selang command to the policy:

```
newres FILE \Device\Mup\*
```

To block users access to network and shared drives on Windows 2003, add the following selang command to the policy:

```
newres FILE \Device\LanmanRedirector\*
```

### **User Can Access Protected Resources**

#### **Symptom:**

I created a default access authority of none for a resource, but the superuser can still access the resource.

#### **Solution:**

[Troubleshoot the resource access problem.](#)

### **Read Access Checks Bypass etc/passwd and etc/group Files**

#### **Valid on UNIX**

##### **Symptom:**

I created a rule that has a default access authority of none for the /etc/passwd and /etc/group files, but I still have read access to these files.

##### **Solution:**

By default, the Privileged Access Manager authorization engine bypasses read access checks for the /etc/passwd and /etc/group system files. To stop Privileged Access Manager bypassing read access checks for system files, change the value of `bypass_system_files` in the `[seosd]` section of the `seos.ini` file to `no`.

##### **WARNING**

If you stop Privileged Access Manager bypassing read access checks for system files, verify that correct authorizations are in place. If you do not set the correct authorizations and bypass read access checks, users including Privileged Access Manager administrations and the root user may not be able to access the system. A critical system processes may fail.

### **An Enterprise User or Group Cannot Access Resources but Correct Access Rules are Set**

#### **Valid on Windows**

##### **Symptom:**

I can see that an enterprise user or group has permissions to access a resource but they cannot access it.

##### **Solution:**

The enterprise account may have been recycled and the permissions in the database apply to the old account, not the new account that has the same name but a different SID. To check for this scenario, resolve recycled enterprise accounts.

##### **NOTE**

For more information about resolving recycled enterprise accounts, see the *Endpoint Administration Guide for Windows*.

### **Failed Login Does Not Lock Out User**

#### **Valid on UNIX**

##### **Symptom:**

I configure `serevu` to disable users in the password PMD after a specified number of failed login attempts. When a user fails to log in correctly, Privileged Access Manager does not lock out the user. When I start `serevu` with the `nodaemon` option to view the `pam_failed_logins.log` file, the server does not respond.

##### **Solution:**

The value of `passwd_pmd` in the `[seos]` section of the `seos.ini` file is incorrect. Set the value of `passwd_pmd` to the name of the password PMD to which `sepass` sends password updates.

### **Users Can Run Commands Outside Time Restrictions**

##### **Symptom:**

I set time restrictions on a group, but group members can run Privileged Access Manager commands outside the permitted times.

##### **Solution:**

During a restricted time period, Privileged Access Manager prevents users from starting a new login session but cannot force users to disconnect. To prevent users from accessing resources or commands in a restricted time period, change the resource record for the resource or command to include time restrictions.

**NOTE**

Privileged Access Manager checks if time restrictions exist in the USER or XUSER record for the user before it checks if time restrictions exist for GROUP or XGROUP to which the user belongs.

## **CA Privileged Access Manager Server Control Recognizes All Users as root**

### **Valid on UNIX**

#### **Symptom:**

When I run the `sewhoami` utility for a non-root user, Privileged Access Manager recognizes the user as root.

#### **Solution:**

To troubleshoot this problem, verify the following in the LOGINAPPL record of the login application:

- The name of the LOGINAPPL record is the name of the login application.
- The LOGINPATH parameter in the LOGINAPPL record specifies the correct, full path to the login application.

**NOTE**

To determine the path to the login application, [run a trace](#) and then use the login application to log in and log out of Privileged Access Manager. Review the trace to obtain the path.

The LOGINSEQUENCE parameter in the LOGINAPPL record specifies the correct login sequence for the login application. For assistance, contact CA Support at <http://ca.com/support>.

**NOTE**

Privileged Access Manager does not define LOGINAPPL records for third-party login applications. If you use a third-party login application, manually define the LOGINAPPL record for the application.

## **Cannot Add User as Password Manager to Only One Group**

#### **Symptom:**

I want to make a user a password manager for a specific group, but when I execute the following command the user becomes a password manager for all groups:

```
editusr userName pwmanager
```

#### **Solution:**

Specify the name of the group to which you want to add the user as a password manager, as follows:

```
join userName group(groupName) pwmanager
```

## **Windows Administrators Can Change Privileged Access Manager Server Control Passwords**

### **Valid on Windows**

#### **Symptom:**

Windows administrators can change Privileged Access Manager passwords in my Privileged Access Manager-protected Windows environment.

#### **Solution:**

To help ensure that only users that you specify in Privileged Access Manager can change passwords, set the value of the EnforceViaTrust registry entry to 1 in the following key:



```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd
```

This registry entry specifies to enforce that you can update or create user passwords through Privileged Access Manager only. The default value of the registry entry is 0, meaning that you do not have to use Privileged Access Manager to update or change a user password.

### **Global Password Policies Lock Users Out of Protected Systems**

#### **Symptom:**

When I implement a global password policy, the password policy locks users out of systems protected by Privileged Access Manager.

#### **Solution:**

Create a separate password policy for the users who must access the Privileged Access Manager-protected system. Use a profile group to create a password policy for these users.

The following process describes how to use a profile group to implement a password policy:

1. Create a profile group.
2. Set the password policy for the profile group.
3. Assign the users to the profile group.

The password policy that you set for the profile group now applies to the users associated with the profile group.

### **Task Delegation Hangs for Interactive Application**

#### **Valid on Windows**

#### **Symptom:**

I write a task delegation rule that lets a user run an interactive Windows application, for example, notepad.exe. When the user tries to run the application, the task delegation hangs.

#### **Solution:**

The interactive flag must be set for the SUDO class record that permits the user to run the application. If you use task delegation to run an interactive Windows application and the interactive flag is not set, the application runs in the background and you cannot interact with it.

To fix this problem, do the following:

1. Set the interactive flag for the SUDO record:

```
er SUDO resourceName interactive
```

#### **– resourceName**

Specifies the name of the resource record that lets the user run the application.

The interactive flag is set for the specified resource.

2. Restart the Task Delegation service, as follows:
  - a. Kill the interactive application.
  - b. If task delegation still hangs, restart Privileged Access Manager.

#### **NOTE**

For more information about task delegation and defining SUDO records, see the *Endpoint Administration Guide for Windows*.

## Manage the CA Privileged Access Manager Server Control Database

### selang Query Returns Maximum of 100 Records

#### Symptom:

When I run a selang query that should return more than 100 records, Privileged Access Manager displays the following message:

```
WARNING: Only 100 (query size limit) items are displayed.
```

#### Solution:

The default value of the query\_size configuration setting is 100. To increase the number of records that Privileged Access Manager returns for selang queries, change the value of the query\_size configuration setting.

The query\_size configuration setting is located in the:

- (UNIX) [lang] section of the seos.ini file
- (Windows) lang subkey, as follows:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang

### UTimes and Denied Records in the Audit Log After Database Backup

#### Symptom:

When Privileged Access Manager is running and I back up the database with my OS backup tools, Privileged Access Manager sends an entry to the audit log similar to the following message:

```
03 Mar 2008 15:58:01 D FILE          UTimes      69 10
/opt/CA/PAMSC/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

#### NOTE

The example above is written using UNIX pathnames, but the solution is also valid for Windows computers.

#### Solution:

The audit message means that Privileged Access Manager prevented the backup operation from updating the UTimes file date stamp. Privileged Access Manager did not prevent the backup itself.

To prevent this message from appearing in the audit log, complete the following tasks:

- If the backup program is executed by a non-superuser, verify that the user has the OPERATOR attribute.
- If the backup program is executed by a superuser, verify that the backup program has a SPECIALPGM record that has the pgmtype (backup) property.

To verify that the database is correctly backed up, use the dbmgr utility to perform the backup.

### The Privileged Access Manager Database Is Corrupt

#### Valid on UNIX

#### Symptom:

I notice messages similar to the following messages in the Privileged Access Manager error log:

```
seoswd: [ID 973226 auth.error] Communication time out to seosd. Executing seosd
FATAL!Inseosrt_InitDatabase (0x270)
WARNING: /Path of Access Control/seosdb/seos_cdf.dat was corrupted
```

**Solution:**

Use the following procedure to fix the database corruption:

**NOTE**

This procedure assumes that the database is installed in the default installation location, /opt/CA/PAMSC

**To fix the Privileged Access Manager database corruption:**

1. Stop Privileged Access Manager:

```
secons -s
```

2. (Optional) Back up the database to another location so that the database can be provided to Technical Support if necessary.

3. Verify that the database is marked as closed:

```
cd /opt/CA/PAMSC/seosdb
dbmgr -util -close
```

**NOTE**

If Privileged Access Manager is not shut down correctly, the database can be marked as open.

4. Check the database:

```
dbmgr -util -check
```

5. Do *one* of the following tasks:

- If you do not receive an error message when you check the database, go to Step 6.
- If you receive an error message when you check the database, do not complete Steps 6 and 7. Instead, [rebuild the database](#).

6. Build the database files:

```
dbmgr -util -build all
```

7. Check the database again:

```
dbmgr -util -check
```

8. Start Privileged Access Manager:

```
seload
```

**Note:** If the database is still corrupt, further investigation is required. For assistance, contact CA Support at <http://ca.com/support>.

## Connecting to Remote Computers

### Cannot Connect to Remote Computer

**Symptom:**

I cannot connect to a remote Privileged Access Manager computer.

**Solution:**

[Troubleshoot the connection problem.](#)

### Communication Time Out to seosd Appears Continuously in syslog

**Valid on Windows****Symptom:**

When I run Privileged Access Manager, the computer occasionally slows down and the following messages appear in syslog:

```
seoswd: Communication time out to seosd. Executing seosd
seoswd: Communication problem with seosd returned 5378 [Success]
seoswd: Description: Timeout communication with seosd.
```

**Solution:**

The antivirus software on the computer causes Privileged Access Manager to time out. Do the following in the antivirus software:

- Exclude the Privileged Access Manager directory from real-time scanning.
- Stop the real-time (on access) scan for the Privileged Access Manager directory.

Because Privileged Access Manager protects the Privileged Access Manager registry keys, files, and installation directory by default, the previous actions should not increase the virus threat to the computer.

We recommend that you create a SPECIALPGM record for the antivirus software. Set the PGMTYPE property to pbf for the SPECIALPGM record. The pbf program type bypasses database checks for file handling events.

**First Incoming ftp Connection Cannot Be Controlled****Valid on UNIX****Symptom:**

When I start Privileged Access Manager, it does not control the first incoming ftp connection from vsftpd. I have created a TCP rule for ftp and a HOST rule for vsftpd, and Privileged Access Manager controls all subsequent incoming ftp connections from vsftpd according to the TCP or HOST rule that I created.

**Solution:**

If you start vsftpd before you start Privileged Access Manager, vsftpd places a hook in the accept system call for incoming ftp connections. The hook means that vsftpd processes the first incoming ftp connection before Privileged Access Manager can intercept it.

After vsftpd processes the ftp connection, it tries to call the accept system call in preparation for the next ftp connection. However, Privileged Access Manager intercepts this system call and hence controls all subsequent ftp connections.

To intercept the first incoming ftp connection, use one of the following workarounds:

- Start Privileged Access Manager before you start vsftp.
- Use a super-server daemon such as inetd or xinetd to start vsftpd.

**NOTE**

For more information about configuring a super-server daemon, contact your OS vendor.

- Run the tripAccept utility after you start Privileged Access Manager.  
To run the tripAccept utility, you must enable the call\_tripAccept\_from\_seload token in the [SEOS\_syscall] section of the seos.ini file. We recommend that you define a SPECIALPGM record for the tripAccept utility before you run it.

**Target Pages on Local Host and Target Host Are Different****Valid on UNIX****Symptom:**

When I try to connect to a Privileged Access Manager host, I get the following message:

```
WARNING: Local machine's code page is different from target host's.
```

**Solution:**

Verify that the locale configuration setting in the [seos] section of the seos.ini file has the same value on the local host and the target host.

## **Cannot Connect to an Endpoint Using selang**

### **Symptom:**

When I try to connect to an endpoint using selang, I receive an error message similar to the following:

```
Unpacking of data failed
```

### **Solution:**

A problem exists with the encryption that is used to protect inter-component communication. Check Privileged Access Manager computers for recent changes to the encryption key and the encryption method.

#### **NOTE**

For more information about encryption methods, see the *Implementation Guide*.

## **Deploy Rules from a PMD**

### **Subscriber PMDB Cannot Receive Updates from the Master PMDB**

#### **Symptom:**

I have a hierarchical PMDB architecture. A subscriber PMDB does not receive updates from the master PMDB. The error log of the master PMDB has the following message:

```
Cannot receive update from non-parent PMDB
```

#### **Solution:**

When a subscriber PMDB does not receive updates from the master PMDB, use the following procedure to troubleshoot the problem.

#### **To troubleshoot PMDB update problems:**

1. List the subscribers of the master PMDB (*master\_pmdb\_name*) and their status:

```
sepmdb -L master_pmdb_name
```

#### **NOTE**

Run this command on the master PMDB computer.

2. Review the list of subscribers to determine which subscribers are unavailable.
3. Verify that the value of the parent\_pmd configuration setting is correct on each unavailable subscriber. The parent\_pmd configuration setting is located in:
  - (UNIX) The [seos] section of the seos.ini and the pmd.ini files
  - (Windows) The following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl
```

**Note:** The hostname that you specify in the parent\_pmd token must match the hostname of the master PMDB exactly. Verifying that hostname resolution is correctly configured may help troubleshoot this issue. If you use a UNIX computer, you can use the sehostinf utility to discover the hostname of the master PMDB. For assistance, contact CA Support at <http://ca.com/support>.

If the problem still exists, do the following:

1. Display the master PMDB error log:
 

```
sepmdb -e master_pmdb_name
```
2. Review the error log and note what error codes are reported for the unavailable subscribers.
3. For each unavailable subscriber, use the error code to troubleshoot the problem.

If the problem still exists, do the following:

1. Remove the problematic subscriber from the list of unavailable subscribers that the master PMDB maintains:

```
sepmdb -r pmdb_name subscriber_name
```

The parent PMDB tries to send updates to the subscriber.

2. Repeat the previous procedure.
3. If there are any changes to the list of subscribers or to the parent PMDB error log, use the changes to troubleshoot the problem.

### **Failed Events in Audit Log of Subscriber Endpoint**

#### **Symptom:**

A subscriber does not receive updates from a master PMDB. I notice *Failed* events in the Privileged Access Manager audit log of the subscriber.

#### **Solution:**

The PMDB user does not have the ADMIN attribute. To give the PMDB user the ADMIN attribute, edit the user record using the following selang command:

```
chusr userName admin
```

#### **NOTE**

You must have the ADMIN attribute to run this selang command. Privileged Access Manager bypasses TERMINAL rules when deploying PMDB updates to subscribers.

## **Collect Audit Records**

### **Some Audit Log Messages Are Not Received by the Collection Server**

#### **Valid on UNIX**

#### **Symptom:**

I configured the endpoints in my Privileged Access Manager installation to route their local audit logs to a central log collection server. However, the server does not receive all the audit logs. I configured selogrd to emit the audit records and selogrd to collect the audit records.

#### **Solution:**

To troubleshoot selogrd, the emitter daemon for the Privileged Access Manager log routing system, follow these steps:

- Review the selogrd.cfg file. This file configures which audit messages Privileged Access Manager routes to the central log collector.
- Review the audit log for each endpoint. If an audit event is missing from the audit log, review the audit.cfg file. The audit.cfg file configures which audit events Privileged Access Manager writes to the audit log. If the audit.cfg file prevents Privileged Access Manager from writing an audit event to the audit log, the audit event cannot be routed.
- Configure selogrd, the emitter daemon for the log routing system, to print debug messages then recreate the problem. Use the following command to configure selogrd to print debug messages:

```
selogrd -d
```

### **No Audit Log Messages Are Received by the Collection Server**

#### **Valid on UNIX**

**Symptom:**

I configured the endpoints in my Privileged Access Manager installation to route their local audit logs to a central log collection server. However, the server does not receive any audit logs. I configured selogrd to emit the audit records and selogrcd to collect the audit records.

**Solution:**

Verify that selogrcd is running on the log collection server.

**NOTE**

If selogrcd does not run for an extended timeframe, audit events may be discarded by the endpoints.

**SID Resolution Failed (Event Viewer Warning)****Valid on Windows****Symptom:**

When I view the Application log of the Windows Event Viewer, I find a Warning event from Privileged Access Manager that says that resolving a specific SID into an account name has failed.

**Solution:**

A *security identifier (SID)* is a numeric value that identifies a user or group to the operating system. Each entry in the discretionary access control list (DACL) has a SID. The SID identifies the user or group for whom access is allowed, denied, or audited.

This warning appears when the operating system was not able to convert the SID into an account name, for example, if the user or group that the SID refers to no longer exists. Ensure that the problematic system and its corresponding domain controller are configured correctly for SID resolution.

**SID Resolution Times Out (Event Viewer Warning)****Valid on Windows****Symptom:**

When I view the Application log of the Windows Event Viewer, I find a Warning event from Privileged Access Manager that says that resolving a specific SID into an account name has timed out.

**Solution:**

A *security identifier (SID)* is a numeric value that identifies a user or group to the operating system. Each entry in the discretionary access control list (DACL) has a SID. The SID identifies the user or group for whom access is allowed, denied, or audited.

This warning appears when the operating system was not able to convert the SID into an account name within the defined timeout. Ensure that the following conditions are true:

- The problematic system and its corresponding domain controller are configured correctly for SID resolution.
- Network settings are configured correctly.

You can also increase the timeout by changing the DefLookupTimeout configuration setting in the following registry key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\SeOSD
```

**NOTE**

Increasing the SID resolution timeout may downgrade Privileged Access Manager performance.

---

## **Receive Error Code 4631 When Attempting to Start selogrd**

### **Valid on UNIX**

#### **Symptom:**

I attempt to start selogrd. selogrd does not start and I receive the following error message:

```
ERROR 4631 (0x1217) initializing /opt/CA/PAMSC/bin/selogrd
```

#### **Solution:**

Resolve the local host name before you start selogrd. To resolve the host name, add the host name to the operating system hosts file, or define the host name to NIS or DNS.

## **Audit Logging Stops When Audit File Size Exceeds 2 GB**

### **Symptom:**

Privileged Access Manager stops writing audit records to the audit file when the audit file size exceeds 2 GB.

#### **Solution:**

Privileged Access Manager cannot write audit records to the audit file when the size of the audit file exceeds 2 GB. The maximum size of the audit file is specified, in KB, by the audit\_size configuration setting in the logmgr section.

To set the maximum size of the seos.audit file to 2 GB, set the value of the audit\_size configuration setting in the logmgr section to 2097151.

## **System Slows When Privileged Access Manager Writes to Audit Log**

### **Symptom:**

My computer slows when Privileged Access Manager writes to the audit log.

#### **Solution:**

Most processes in the system could be blocked while Privileged Access Manager writes audit and trace data. To reduce the time it takes to write audit data and trace data, do the following:

- Set the audit mode only for resources and accesses you need.
- Open the trace only when you need to.
- Store audit file, trace file, and Privileged Access Manager database files on the fastest available file system.

## **Filter Not Applied If Host Is Assigned Multiple IP Addresses**

### **Symptom:**

I configured the audit.cfg to filter TCP events on a host that is assigned multiple IP addresses using the host name. After I applied the filter, I cannot see the TCP logs for all the IP addresses.

#### **Solution:**

When you apply the audit.cfg filter, the audit system resolves the host name to the IP address of the host and the host IP address to the host name. If you configure the host with more than one IP address, the audit.cfg filters the first IP address only.

To apply the audit.cfg filter to all IP addresses, specify all the IP addresses in the filter only and not the host name.

Example:



```
TCP;*;192.168.30.138;*;R;P
```

```
TCP;*;192.168.30.139;*R;P
```

## PAM SC reference

This section provides reference material for PAM Server Control.

Use the table of contents to access the topics in this section.

### Configuration Files

- [audit.cfg File Filter Audit Records](#)
- [auditrouteft.cfg File Filter Audit Records Routing](#)
- [The accommon.ini File](#)
- [The Audit Log Route Configuration File selogrd.cfg](#)
- [The lang.ini File](#)
- [The pmd.ini File](#)
- [The seos.ini Initialization File](#)
- [The uxauth.ini File](#)
- [trcfilter.init](#)

### audit.cfg File Filter Audit Records

The audit.cfg file filters audit records on a host by defining records that are not sent to the audit file. Each line represents a rule for filtering out audit information.

By default, the audit.cfg file is located in the following directories:

- (UNIX) /opt/CA/PAMSC/etc
- (Windows) C:\Program Files\CA\PAMSC\data

You can change the location of the audit.cfg file by editing the [logmgr] AuditFiltersFile token in the seos.ini file (UNIX), or the AuditFiltersFile entry in the logmgr registry key (Windows).

#### NOTE

Save the audit.cfg file using UTF-8 encoding if you filter the file that includes Japanese characters.

Use the audit.cfg file to filter out records in the following audit event types, each type by a different syntax:

- resource access
- [network connection](#)
- [login and logout events](#)
- [security database administration](#)
- trace message on a user

#### NOTE

A \* in any column in each type of syntax stands for "any value".

## audit.cfg File Resource Access Events Filter Syntax

Audit records that belong to a resource access event have the following filter format:

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

- **ClassName**  
Defines the name of the class that the accessed object belongs to.

### NOTE

Enter the name of the class in uppercase.

- **ObjectName**  
Defines the name of the object that was accessed.
- **UserName**  
Defines the name of the accessor.
- **ProgramPath**  
Defines the name of the program used to access the object.
- **Access**  
Defines the requested access to the object.

### NOTE

The following values are the values for this parameter that you use in the audit.cfg file to filter out an audit record. In some cases the value of this parameter in the audit.cfg file is different to the value that Privileged Access Manager writes in the audit record for that event. Any such differences are noted after the description of each value. Type the parameter in the same case as it appears in the following list.

### NOTE

#### Values:

- **\***  
A wildcard that represents any type of access.
- **Chdir**  
Change directory The accessor made a request to move the object to a different directory.
- **Chmod**  
Change mode The accessor made a request to change the mode of the object.
- **Chgrp**  
(UNIX) Change group The accessor made a request to change the group the object belongs to.
- **Chown**  
Change owner The accessor made a request to change the owner of the object.
- **Connect**  
Join user to group The accessor made a request to add a new user to a group.  
**Note:** The connect value is identical to the join value.
- **Control**  
(UNIX) Control The accessor requested Chown, Chmod, Utime, Sec, Chdir, and Update access to the object.
- **Cre**  
Create The accessor made a request to create an object.

### NOTE

#### Crdrwr

#### Crread

Create and Read The accessor requested Create and Read access to the object.

**Note:** Privileged Access Manager writes this value as CrRead in the corresponding audit record.

#### Crwrite

Create and Write The accessor requested Create and Write access to the object.

Note: Privileged Access Manager writes this value as CrWrite in the corresponding audit record.

– **Del**

DeleteThe accessor made a request to delete an object.

**NOTE**

Privileged Access Manager writes this value as Erase in the corresponding audit record.

– **Join**

Join user to groupThe accessor made a request to add a new user to a group.

**NOTE**

The join value is identical to the connect value.

– **Kill**

Kill The accessor made a request to kill a process.

Modify

Modify The accessor requested Modify access to the object.

OwnGrp

Change owner and Change groupThe accessor requested Chown and Chgrp access to the object.

**NOTE**

PW

– **R**

ReadThe accessor requested read access to an object.

**NOTE**

(UNIX) If STAT\_intercept is set to 1, this parameter includes *stat* interception.

– **Rename**

Change file nameThe accessor made a request to change the file name of an object.

– **Sec**

Change ACLThe accessor made a request to edit the ACL of the object.

**NOTE**

Privileged Access Manager writes this value as ACL in the corresponding audit record.

**Update**

Read, Write, and ExecuteThe accessor requested Read, Write, and Execute access to an object.

Note: The Update value also filters events when an accessor requested Read and Write access to an object.

– **Utime**

(UNIX)Change timeThe accessor made a request to change the modification time of an object.

**NOTE**

Privileged Access Manager writes this value as Utimes in the corresponding audit record.

– **W**

WriteThe accessor requested write access to an object.

– **X**

ExecuteThe accessor made a request to execute an object.

**NOTE**

Some values are not valid for every class. For example, kill is an invalid value for the FILE class, because the kill action is not available to objects in the FILE class. If you enter an invalid value for a class when you write a rule, Privileged Access Manager ignores that rule when it reads the file.

• **AuthorizationResult**

Defines the authorization result.

**Values:**

P - Permitted

D - Denied

O - Logout

I - Inactivate (Disable user) by serevu

E - Enable user login by serevu

A - Password attempt detected

\* - A wildcard that represents any value

### Example: Audit Filter Policy

- This example shows you what an audit filtering policy looks like:

```
env config
er config audit.cfg line+("FIEL;*;*;*;R;P")
```

- This policy writes the following line to the audit.cfg file. The line filters audit records that record a permitted attempt by any accessor to access any file resource for reading:

```
FILE;*;*;*;R;P
```

### audit.cfg File Network Connection Events Filter Syntax

Audit records that belong to a network connection event have the following filter format:

```
{HOST|TCP};ObjectName;HostName;ProgramPath;Access;AuthorizationResult
```

- HOST**  
Specifies that the rule filters records generated by objects in HOST class, that is, incoming TCP connections.
- TCP**  
Specifies that the rule filters records generated by objects in TCP class, that is, connect with service events.
- ObjectName**  
Defines the name of the object that was accessed. *ObjectName* can be a service name or port number.
- HostName**  
Defines the name of the host. *HostName* must be an object in the HOST class.
- ProgramPath**  
Defines the login program type.  
(Windows) For outgoing connections, this parameter defines the program path of the process trying to establish the connection.

#### NOTE

This parameter has no meaning for incoming connection events. Use \* for this parameter to filter audit records generated by incoming connection events.

- Access**  
Defines the type of attempted connection.

#### NOTE

##### Values:

- (HOST) \*
- (TCP) R (incoming connection), W (outgoing connection), \*

- AuthorizationResult**  
Defines the authorization result.  
**Values:** P (permitted), D (denied), \*

### Examples: Filter Network Connection Events

- This example filters all audit records from the host ca.com generated by successful incoming telnet connections:

```
HOST;telnet;ca.com;*;*;P
```

- This example filters all audit records from the host ca.com generated by incoming and outgoing login TCP connections that were denied:

```
TCP;login;ca.com;*;*;D
```

- This example filters all audit records from the host ca.com generated by outgoing telnet connections:

```
TCP;telnet;ca.com;*;W;*
```

## audit.cfg File Login and Logout Events Filter Syntax

Audit records that belong to a login or logout event have the following filter format:

```
LOGIN;UserName;UserId;TerminalName;LoginProgram;AuthorizationResultOrLoginType
```

- **LOGIN**  
Specifies that the rule filters audit records generated by login and logout events.
- *UserName*  
Defines the name of the accessor.
- *UserId*  
(UNIX) Defines the native user ID of the accessor.
- *TerminalName*  
Defines the terminal at which the event occurred.
- *LoginProgram*  
Defines the name of the program that attempted to log in or out.
- *AuthorizationResultOrLoginType*  
Defines the authorization result.

### NOTE Values:

- \*  
A wildcard that represents any type of authorization result.
- **D**  
The login attempt was denied.
- **P**  
The login attempt was permitted.
- **O**  
(UNIX) The accessor logged out.
- **I**  
(UNIX) The serevu daemon revoked the accessor's account.
- **E**  
(UNIX) The serevu daemon enabled the accessor's account.
- **A**  
(UNIX) The serevu daemon or Pluggable Authentication Module audited a user's attempt to log in with an incorrect password.

### NOTE Windows does not record logout events.

## Examples: Filter Login or Logout Events

- This example filters all audit records generated when root logs in to a permitted account:

```
LOGIN;root;*;*;*;P
```

- This example filters all audit records generated when root logs in successfully due to the system's CRON program:

```
LOGIN;root;*;*;SBIN_CRON;P
```

- This example filters all audit records generated when the `_CRONJOB_` process logs the root user out:

```
LOGIN;root;*;*_CRONJOB_*;O
```

## audit.cfg File Security Database Administration Events Filter Syntax

Audit records that belong to a security database administration event have the following filter format:

```
ADMIN;ClassName;ObjectName;UserName;EffectiveUserName;TerminalName;Command;CommandResult
```

- **ADMIN**  
Specifies that the rule filters audit records generated by events performed by an administrator.
- *ClassName*  
Defines the class on which the administrator executes the command.
- *ObjectName*  
Defines the object that the administrator's command updated.
- *UserName*  
Defines the name of the user who executed the command.
- *EffectiveUserName*  
(UNIX) Defines the name of the effective user to which the rule applies.  
(Windows) Defines the name of the native user to which the rule applies.
- *TerminalName*  
Defines the terminal at which the event occurred.
- *Command*  
Defines the command that the administrator executed.
- *CommandResult*  
Defines the authorization or command result.

### NOTE

**Values:** S (command succeeded), F (command failed), D (command denied), \*

### Example: Filter Security Database Administration Events

This example filters all audit records generated by successful FILE management commands by admin01:

```
ADMIN;FILE'*;admin01;*;*;S
```

## audit.cfg File Trace Messages On a User Events Filter Syntax

Audit records that belong to a trace message on a user event have the following filter format:

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;AuthorizationResult;TraceMessage
```

### NOTE

The maximum limit for the trace filter is 1000 records.

- **TRACE**  
Specifies that the rule filters user trace records.
- *TracedClassName*  
Defines the name of the object class the user tried to access.

### NOTE

Enter the name of the class in uppercase.

- *TracedObjectName*

Defines the name of the object that the user tried to access.

- **RealUserName**  
(UNIX) Defines the name of the real user that generated the trace record.  
(Windows) Defines the name of the native user that generated the trace record.
- **EffectiveUserName**  
(UNIX) Defines the name of the effective user that generated the trace record.  
(Windows) Defines the name of the native user that generated the trace record. This parameter is identical to the RealUserName parameter. Use \* for this parameter.
- **ACUserName**  
Defines the user name Privileged Access Manager chose to authorize the event.
- **AuthorizationResult**

#### NOTE

Defines the authorization result. Values: P (permitted), D (denied), \*

- **TraceMessage**  
Defines the trace message that was generated.

### Example: Filter Trace On a User Message Events

This example filters all user trace records generated when the effective user is root, and root accessed an object in the FILE class:

```
TRACE;FILE;*;*;root;*;*;*
```

## auditrouteflt.cfg File Filter Audit Records Routing

The auditrouteflt.cfg file filters audit records routing by defining records that Privileged Access Manager should not send to the Distribution Server. Each line represents a rule for filtering out audit information. The file pathname is defined by the audit\_filter configuration setting in the ReportAgent section.

#### NOTE

Filtered audit events are written to the local audit file but Privileged Access Manager does not send them to the message queue on the Distribution Server. To filter out audit messages from the local audit file, modify filter rules in the file defined by the AuditFiltersFile configuration setting in the logmgr section (by default, audit.cfg).

You can use the auditrouteflt.cfg file to filter out records in the following audit event types, each type by a different syntax:

- resource access
- network connection
- login and logout events
- security database administration
- trace message on a user

#### NOTE

A \* in any column in each type of syntax stands for "any value".

### Resource Access Events Filter Syntax

Audit records that belong to a resource access event have the following filter format:

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

- **ClassName**  
Defines the name of the class that the accessed object belongs to.

#### NOTE

You must enter the name of the class in uppercase.

- **ObjectName**

Defines the name of the object that was accessed.

- *UserName*  
Defines the name of the accessor.
- *ProgramPath*  
Defines the name of the program used to access the object.
- *Access*  
Defines the requested access to the object.

#### **NOTE**

##### **Values:**

- **\***  
A wildcard that represents any type of access.
- **Chdir**  
Change directoryThe accessor made a request to move the object to a different directory.
- **Chmod**  
Change modeThe accessor made a request to change the object's mode.
- **Chgrp**  
(UNIX) Change groupThe accessor made a request to change the group the object belongs to.
- **Chown**  
Change ownerThe accessor made a request to change the owner of the object.
- **Cre**  
CreateThe accessor made a request to create a new object.
- **Del**  
DeleteThe accessor made a request to delete an object.
- **Join**  
Join user to groupThe accessor made a request to add a new user to a group.
- **Kill**  
KillThe accessor made a request to kill a process.
- **R**  
ReadThe accessor requested read access to an object.

#### **NOTE**

(UNIX) This parameter includes *stat* interception if STAT\_intercept is set to 1.

- **Rename**  
Change file nameThe accessor made a request to change the file name of an object.
- **Sec**  
Change ACLThe accessor made a request to edit an object's ACL.
- **Utime**  
(UNIX) Change timeThe accessor made a request to change the modification time of an object.
- **W**  
WriteThe accessor requested write access to an object.
- **X**  
ExecuteThe accessor made a request to execute an object.

#### **NOTE**

Some values are not valid for every class. For example, kill is an invalid value for the FILE class, because the kill action is not available to objects in the FILE class. If you enter an invalid value for a class when you write a rule, Privileged Access Manager ignores that rule when it reads the file.

- *AuthorizationResult*  
Defines the authorization result.



**NOTE**

**Values:** P (permitted), D (denied), \*

**Network Connection Events Filter Syntax**

Audit records that belong to a network connection event have the following filter format:

```
{HOST|TCP};ObjectName;HostName;ProgramPath;Access;AuthorizationResult
```

- **HOST**

Specifies that the rule filters records generated by objects in HOST class, that is, incoming TCP connections.

- **TCP**

Specifies that the rule filters records generated by objects in TCP class, that is, connect with service events.

- *ObjectName* Defines the name of the object that was accessed. *ObjectName* can be a service name or port number.

- *HostName*

Defines the name of the host. *HostName* must be an object in the HOST class.

- *ProgramPath*

Defines the login program type.

(Windows) For outgoing connections, this parameter defines the program path of the process trying to establish the connection.

**NOTE**

This parameter has no meaning for incoming connection events. Use \* for this parameter to filter audit records generated by incoming connection events.

- *Access*

Defines the type of attempted connection.

**NOTE**

**Values:**

- (HOST) \*
- (TCP) R (incoming connection), W (outgoing connection), \*

- *AuthorizationResult*

Defines the authorization result.

**NOTE**

**Values:** P (permitted), D (denied), \*

**Login and Logout Events Filter Syntax**

Audit records that belong to a login or logout event have the following filter format:

```
LOGIN;UserName;UserId;TerminalName;LoginProgram;AuthorizationResultOrLoginType
```

- **LOGIN**

Specifies that the rule filters audit records generated by login and logout events.

- *UserName*

Defines the name of the accessor.

- *UserId*

Defines the native user ID of the accessor.

- *TerminalName*

Defines the terminal at which the event occurred.

- *LoginProgram*

Defines the name of the program that attempted to log in or out.

- *AuthorizationResultOrLoginType*

Defines the authorization result.

**NOTE****Values:**

- **\***  
A wildcard that represents any type of authorization result.
- **D**  
The login attempt was denied.
- **P**  
The login attempt was permitted.
- **O**  
(UNIX) The accessor logged out.
- **I**  
(UNIX) The serevu daemon revoked the accessor's account.
- **E**  
(UNIX) The serevu daemon enabled the accessor's account.
- **A**  
(UNIX) The serevu daemon or Pluggable Authentication Module audited a user's attempt to log in with an incorrect password.

**NOTE**

Windows does not record logout events.

**Security Database Administration Events Filter Syntax**

Audit records that belong to a security database administration event have the following filter format:

```
ADMIN;ClassName;ObjectName;UserName;EffectiveUserName;TerminalName;Command;CommandResult
```

- **ADMIN**  
Specifies that the rule filters audit records generated by events performed by an administrator.
- *ClassName*  
Defines the class on which the administrator executes the command.
- *ObjectName*  
Defines the object that the administrator's command updated.
- *UserName*  
Defines the name of the user who executed the command.
- *EffectiveUserName*  
(UNIX) Defines the name of the effective user to which the rule applies.  
(Windows) Defines the name of the native user to which the rule applies.
- *TerminalName*  
Defines the terminal at which the event occurred.
- *Command*  
Defines the selang command that the administrator executed.
- *CommandResult*  
Defines the authorization or command result.

**NOTE**

**Values:** S (command succeeded), F (command failed), D (command denied), \*

**Trace Messages On a User Events Filter Syntax**

Audit records that belong to a trace message on a user event have the following filter format:

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;AuthorizationResult;TraceMessage
```

- **TRACE**

Specifies that the rule filters user trace records.

- *TracedClassName*  
Defines the name of the object class the user tried to access.

#### NOTE

You must enter the name of the class in uppercase.

- *TracedObjectName*  
Defines the name of the object that the user tried to access.
- *RealUserName*  
(UNIX) Defines the name of the real user that generated the trace record.  
(Windows) Defines the name of the native user that generated the trace record.
- *EffectiveUserName*  
(UNIX) Defines the name of the effective user that generated the trace record.  
(Windows) Defines the name of the native user that generated the trace record. This parameter is identical to the RealUserName parameter. Use \* for this parameter.
- *ACUserName*  
Defines the user name Privileged Access Manager chose to authorize the event.
- *AuthorizationResult*  
Defines the authorization result.

#### NOTE

**Values:** P (permitted), D (denied), \*

- *TraceMessage*  
Defines the trace message that was generated.

### Examples: Filter Network Connection Events

- This example filters all audit records from the host ca.com generated by successful incoming telnet connections:  
`HOST;telnet;ca.com;*;*;P`
- This example filters all audit records from the host ca.com generated by incoming and outgoing login TCP connections that were denied:  
`TCP;login;ca.com;*;*;D`
- This example filters all audit records from the host ca.com generated by outgoing telnet connections:  
`TCP;telnet;ca.com;*;W;*`

### Examples: Filter Login or Logout Events

- This example filters all audit records generated when root logs in to a permitted account:  
`LOGIN;root;*;*;P`
- This example filters all audit records generated when root logs in successfully due to the system's CRON program:  
`LOGIN;root;*;*;SBIN_CRON;P`
- This example filters all audit records generated when the \_CRONJOB\_ process logs the root user out:  
`LOGIN;root;*;_CRONJOB_;*;O`

### Example: Filter Security Database Administration Events

This example filters all audit records generated by successful FILE management commands by admin01:

```
ADMIN;FILE'*;admin01;*;*;S
```

### Example: Filter Trace On a User Message Events

This example filters all user trace records generated when the effective user is root, and root accessed an object in the FILE class:

```
TRACE;FILE;*;*;root;*;*;*
```

## Example: Audit Filter Policy

This example shows you what an audit filtering policy looks like:

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

This policy writes the following line to the auditrouteflt.cfg file:

```
FILE;*;*;R;P
```

This line filters audit records that record a permitted attempt by any accessor to access any file resource for reading.

## The accommon.ini File

The accommon.ini configuration file contains tokens that control the initialization process of the Report Agent and tokens that control general communication settings. Example: UNAB registration settings with Privileged Access Manager.

The accommon.ini file is divided into the following sections:

Section	Description
AccountManager	Contains tokens that control the Agent Manager settings
communication	Contains tokens that control general communication settings
global	Contains Privileged Access Manager global settings
ReportAgent	Contains tokens that control the Report Agent settings
AgentManager	Contains tokens that control the Agent Manager settings
DiscoveryAgent	Contains tokens that control the Discovery Agent settings
PupmAgent	Contains tokens that control the Pupm Agent settings

## AccountManager

In the [AccountManager] section, the tokens control the behavior of the Account Manager plug-in.

- **INSTALL\_ACCOUNT\_MNG**

Specifies whether to configure Account Management on the endpoint.

**Values:** Yes, No

**Default:** No

**Example:** INSTALL\_ACCOUNT\_MNG="no"

**NOTE**

Configure the Distribution Server parameters to activate the AccountManager.

- **Interval**

Specifies the AccountManager plug-in interval in seconds.

**Default:** 300

**NOTE**

Applicable if you set the ScheduleType control value to 2.

- **JCS\_USER\_DN**

Specifies the Java Connector Server (JCS) administrator user DN.

**Values:** DN format string

**Default:** cn=root,dc=etasa

**Example:** JCS\_USER\_DN="cn=root,dc=etasa"

- **JCS\_USER\_PSSWD**

Specifies the JCS administrator password.

**Values:** any string.

**Default:** no default value.

**Note:** Asterisks (\*) replace the JCS\_USER\_PSSWD value after installation.

- **JCS\_SERVER\_DN**

Specifies the JCS server DN.

**Values:** DN format string

**Default:** dc=im,dc=etas

**Example:** JCS\_SERVER\_DN="dc=im,dc=etasa"

- **JCS\_SERVER\_PORT**

Specifies the JCS port.

**Values:** Port number

**Default:** 20411

**Example:** JCS\_SERVER\_PORT=20411

- **JCS\_SSL**

Defines the JCS communication protocol.

**Values:** 'yes' for SSL connection, otherwise 'no'.

**Default:** yes

**Example:** JCS\_SSL="yes"

- **max\_threads\_count**

Defines the number of working threads in the pool.

**Values:** 50

- **OperationMode**

Defines whether the AccountManager plug-in is enabled or disabled.

**Options:** 1plug-in enabled, 0plug-in disabled

**Default:** 1

- **PluginPath**

Defines the full pathname of the AccountManager plug-in.

**Default:** /opt/CA/PAMSCShared/lib/AccountManager.so

- **QueryFilter**

Specifies a custom value to add to the Message Queue receive queue filter.

**Options:**

- "ENDPOINT\_CUSTOM1="

a. "ENDPOINT\_CUSTOM2="

b. "ENDPOINT\_CUSTOM3="

c. "ENDPOINT\_CUSTOM4="

d. "ENDPOINT\_CUSTOM5="

e. "ENDPOINT\_OWNER="

f. "ENDPOINT\_DEPARTMENT="

**Default:** no value

**NOTE**

You can use more than one custom property, using the AND operand. Example:

"ENDPOINT\_DEPARTMENT='Finance' AND 'ENDPOINT\_CUSTOM1=Accounting'"

**WARNING**

When specifying the custom property, verify that:

- You use apostrophes to specify the property value.
- You use the AND, OR operands when specifying more than one property.
- You use the parenthesis when using the OR operand.

- **Schedule**

Specifies the AccountManager plug-in a schedule string.

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

#### **NOTE**

Applicable if you set the ScheduleType control value to 3.

- **ScheduleType**  
Defines the AccountManager plug-in scheduling type.  
**Options:**
  - 0 Run once
  - 1 Run on demand
  - 2 Run every N seconds
  - 3 Run according to the scheduling string: 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat**Default:** 2

## **Communication (accommon.ini)**

In the [communication] section, the tokens control the communication and encryption options.

- **Distribution\_Server**  
Defines the Distribution Server URL. You can define more than one Distribution Server in a comma-separated list.  
**Example:** ssl://ds.comp.com:61616, ssl://ds\_dr.comp.com:61616  
**Default:** None
- **endpoint\_to\_server\_queue**  
Defines the name of the message queue that the endpoint uses to send information to Privileged Access Manager Enterprise Management.  
**Default:** ac\_endpoint\_to\_server
- **jvm\_gc**  
Defines the optional parameter for tuning the Garbage Collector. The JVM uses this parameter while communicating with the Distribution Server.  
**Values:** A string representing complete GC tunables  
**Example:** jvm\_gc = -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
**Default:** Empty value
- **jvm\_ms**  
Defines the optional parameter for the JVM initial heap size -Xms. The JVM uses this parameter while communicating with the Distribution Server.  
**Values:** The size is measured in MB.  
**Example:** jvm\_ms = 512  
**Default:** 0
- **jvm\_mx**  
Defines the optional parameter for a Java virtual machine (JVM) maximum heap size -Xmx. The JVM uses this parameter while communicating with the Distribution Server.  
**Value:** The size is measured in MB.  
**Example:** jvm\_mx = 1024  
**Default:** 0
- **jvm\_ps**  
Defines the optional parameter for the JVM permgen size -XX:MaxPermSize. The JVM uses this parameter while communicating with the Distribution Server.  
**Values:** The size is measured in MB.  
**Example:** jvm\_ps = 128  
**Default:** 0
- **server\_to\_endpoint\_broadcast\_queue**  
Defines the name of the message queue that Privileged Access Manager Enterprise Management uses to broadcast messages to all endpoints.

- Default:** ac\_server\_to\_endpoint\_broadcast
- **server\_to\_server\_broadcast\_queue**  
Defines the name of the message queue that the Enterprise Management Server uses to broadcast topics and authenticate using the reportserver user.  
**Default:** ac\_server\_to\_server\_broadcast
- **server\_to\_server\_queue**  
Defines the name of the message queue that the Enterprise Management Server uses to send messages and authenticate using the reportserver user.  
**Default:** ac\_server\_to\_server
- **ac\_server\_to\_endpoint\_queue**  
Defines the name of the message queue that Privileged Access Manager Enterprise Management uses to send messages to the endpoint.  
**Default:** ac\_server\_to\_endpoint
- **ServerVersion**  
Defines the Distribution Server version for forward compatibility.  
**Example:** 12.01.0648  
**Default:** None
- **ssl\_expected\_hostname**  
Specifies the expected server hostname. The client expects this name in the certificate of the server  
**Default:** None
- **ssl\_keystore**  
Defines the keystore location and the location of the client SSL certificate.  
**Limits:** The full pathname to the keystore location  
**Default:** None
- **ssl\_noverifyhost**  
Specifies whether to enable verification of the host certificate.  
**Limits:** 0, disable host certificate verification; 1, enable host certificate verification  
**Default:** 0
- **ssl\_noverifyhostname**  
Specifies whether to enable verification of the host name.  
**Limits:** 0, disable host name verification; 1, enable host name verification  
**Default:** 0
- **ssl\_truststore**  
Defines the truststore for server verification.  
**Limits:** The full pathname to the truststore  
**Default:** None

## global

In the [global] section, the tokens control the behavior of the Privileged Access Manager endpoint.

- **accommon\_path**  
Specifies the full path name of the acccommon directory.  
**Default:** /opt/CA/PAMSCShared/
- **AC\_Version**  
Defines the version of Privileged Access Manager installed on the endpoint.  
**Default:** none
- **java\_home**  
(Linux s390) Defines the path to the Java libraries.  
**Example:** For an IBM J2SE version 5.0 JRE installed on a Linux390 computer: /opt/ibm/java2-s390-50/jre  
**Default:** none

## ReportAgent

In the [ReportAgent] section, the tokens control the behavior of the Report Agent daemon (ReportAgent).

- **audit\_enabled**  
Specifies whether you want to send endpoint audit data to the Distribution Server.  
**Values:** 0 no; 1 yes  
**Default:** 0
- **audit\_filter**  
Defines the full pathname to the file that contains filtering rules for audit records that the Report Agent routes to an external source (such as the Audit Log). This file determines which records the Report Agent routes.  
**Default:** *ACSharedDir/etc/auditrouteflt.cfg*
- **audit\_queue**  
Defines the name of the queue to which the Report Agent sends endpoint audit data.  
**Default:** queue/audit
- **audit\_read\_chunk**  
Defines the maximal audit records the Report Agent tries to collect in a single read of the audit files.  
**Limits:** A positive integer  
**Default:** 300
- **audit\_send\_chunk**  
Defines the maximal audit records that the Report Agent sends to the Distribution Server in each connection. When the number of audit records the Report Agent collects reaches this number, it sends these records to the Distribution Server.  
**Limits:** A positive integer  
**Default:** 1800
- **audit\_sleep**  
Define the length of time the Report Agent sleeps between generating audit reports.  
**Limits:** A positive integer representing a number of seconds  
**Default:** 10
- **audit\_timeout**  
Defines the cycle at which the Report Agent must send endpoint audit data to the Distribution Server. If this amount of time passes from the last send, the Report Agent sends audit data to the Distribution Server. The Report Agent sends this data even if the number of records it collected is less than the audit\_send\_chunk value.  
**Limits:** A positive integer representing a number of seconds  
**Default:** 300
- **Debug**  
Specifies whether the Report Agent logs debug information.  
If you specify yes (1), the Report Agent logs the following reports:
  - Privileged Access Manager reports to *ACSharedDir/log/ac2xml.log*
  - UNAB reports (uxauthd) to *ACSharedDir/log/unab2xml.log*
  - Privileged Access Manager audit reports that are sent to the Audit Log to *ACSharedDir/log/ac2elm.log*
  - UNAB audit reports that are sent to the Audit Log to *ACSharedDir/log/unab2elm.log*
  - Keyboard Logger reports that are sent to the Audit Log to *ACSharedDir/log/kbl2elm.log***Limits:** 0, Report Agent does not log debug information; 1, Report Agent logs debug information  
**Default:** 0
- **elm\_event\_interval**  
Defines the interval in seconds, at which the Report Agent sends user sessions audit events to the Audit Log.  
**Limits:** 0; no interval, send audit events when messages size exceeds the value specified in the elm\_max\_msg\_size token; any positive integer.  
**Default:** 60
- **elm\_max\_msg\_size**



Defines the maximum size of Keyboard Logger messages, in bytes, that the Report Agent sends to the Audit Log.

**Value:** Any positive integer

**Default:** 300000

- **interval**

Defines the interval, in minutes, at which Privileged Access Manager generates and sends reports to the Distribution Server.

The *schedule* setting defines the interval start time and the days it operates on. If the Report Agent starts later than a scheduled occurrence, it sends a report at the next calculated interval (from the schedule) and then at the defined intervals after that on scheduled days.

**Example:** If you have *schedule=8:30@Mon,Tue, Wed*, and *interval=5* and the Report Agent loads on Tuesday at 8:47 am, the Report Agent generates and sends a report at 8:50 am. This is the earliest cycle calculated from the scheduled start using the 5-minute interval.

**Values:** 0 No interval (use scheduled occurrences only); *positive integer* number of minutes to use as interval

**Default:** 0

- **reportagent\_enabled**

Specifies whether reporting is enabled (1) on the local computer.

**Default:** 0

- **schedule**

Defines when reports are generated and sent to the Distribution Server.

You specify this setting in the following format: *time@day[,day2][...]*

For example, "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

- **send\_queue**

Defines the name of the reporting queue on the Distribution Server to which the Report Agent sends snapshots of the local database and any PMDBs.

**Default:** queue/snapshots

- **restart\_enabled**

Specifies restart of the ReportAgent daemon. Specify 1 to enable the restart.

**Default:** 0

## AgentManager

In the [AgentManager] section, Privileged Access Manager controls the behavior of plug-ins.

```
Plugins = DiscoveryAgent
```

## DiscoveryAgent

In the [DiscoveryAgent] section, the tokens control the behavior of the Discovery Agent plug-in.

- **Interval**

Defines the plugin schedule in seconds.

**Default:** 600

**Note:** Applicable only when *ScheduleType* is set to 2.

- **max\_threads\_count**

Defines the threadpool threads count.

**Default:** 10

- **OperationMode**

Defines the plugin operation mode.

**Options:** 0 - plugin disabled, 1 - plugin enabled

**Default:** 0

- **PluginPath**

Defines the full pathname of the plugin.

**Default:** /opt/CA/PAMSCShared/lib/DiscoveryAgent.\*

- **QueryFilter**

Defines an additional value that is added to receive the message queue filter.

**Default:** empty value

- **Schedule**

Defines the plugin scheduling string.

**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

**Note:** Applicable only when ScheduleType is set to 2.

- **ScheduleType**

Defines the plugin schedule type.

**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule

**Default:** 0

## PupmAgent (accommon.ini)

In the [PupmAgent] section, the tokens control the behavior of the Pupm Agent plug-in.

- **OperationMode**

Defines the plugin operation mode.

**Options:** 0 - plugin disabled, 1 - plugin enabled

**Default:** 0

- **PluginPath**

Defines the full pathname of the plugin.

**Default:** /opt/CA/PAMSCShared/lib/PupmAgent.[so|sl|o]

- **ScheduleType**

Defines the plugin schedule type.

**Options:** 0 - Execute once, 1 - Execute on demand, 2 - Execute every *n* seconds (*n* is defined in the **Interval** token), 3 - Execute by scheduler *string* (*string* is defined in the **Schedule** token). Example:

00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

**Default:** 1

- **Interval**

Defines the plugin interval in seconds, when using **ScheduleType** = 2.

**Default:** 1

- **RegistrationInterval**

Defines the registration lifetime in days.

**Default:** 7

- **Schedule**

Defines the plugin scheduling string, when using **ScheduleType** = 3

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

- **AutoRegister**

Specifies whether to send a registration message to the server on agent startup.

**Options:** 0 - The Pupm agent does not send a registration message to the server, 1 - The Pupm agent sends a registration message to the server.

**Default:** 1

## The Audit Log Route Configuration File selogrd.cfg

Valid on UNIX

The following code is the format of the configuration file, followed by a detailed explanation.

```
section-name-1
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
section-name-2
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
...
```

- **Specifying Audit Records**

The configuration file is a list of which audit records to route-and which not to route-to various destinations. To specify audit records, you describe the contents of one or more particular fields. You can use the standard UNIX pattern matching (the wildcards \* and ?).

For example, to specify records that deal with users whose user names begin with the letters dbms, enter the following code:

```
User(dbms*)
```

This example matches users with names like dbms1, dbms\_mgr, and so on.

To specify the same users, but only the records that deal with their login attempts, enter:

```
User(dbms*) Class(LOGIN)
```

**NOTE**

When a line specifies records in terms of more than one field, it specifies only the records that match *all* those fields.

At the beginning of the same line that specifies the records, specify whether you want the records included or excluded. For example, to include those records in the routing enter the following code:

```
include User(dbms*) Class(LOGIN).
```

This type of line appears in the overall format as:

```
[{include|exclude} match-field(match-pattern) ... .]
```

Here, the ... means that the first match-field(match-pattern) pair can be followed by further pairs.

You can use any of the following for match-field(match-pattern):

- **Access(access-type)**  
For the type of access required; *access-type* is any one of the following:  
ACL, Chdir, Chgrp, Chmod, Chown, Connect, Control, Create, Erase, Exec, Kill, Modify, Owngrp, Password, Read, Rename, Replace, Update, Utimes, and Write.
- **Class(LOGIN)**  
For login records.
- **Class(LOGOUT)**  
For logout records.
- **Class(PWCHANGE)**  
For password administration.
- **Class(HOST)**  
For TCP/IP records.
- **Class(UPDATE CA ControlMinder-class)**  
For database administration. CA ControlMinder-class is any of the accessor or resource classes (such as USER, GROUP, FILE, HOSTNP...) or a pattern for the class name to match. Thus for all database administration, you can specify UPDATE \*.
- **Class(CA ControlMinder-class)**

For access to protected resources. For example, Class(FILE) refers to records reporting file access attempts. You can use an asterisk to combine Class(CA ControlMinder-class) and Class(UPDATE CA ControlMinder-class) as Class(\*CA ControlMinder-class). For example, specifying Class(\*FILE) is like specifying both Class(FILE) and Class(UPDATE FILE). It refers both to attempts to access files and to attempts to update records in the FILE class.

– **Code(return-code)**

For the Privileged Access Manager return code indicating what happened; return-code can take the following values. (See also Example 1 in this section.)

**A**-An attempt to log in failed because an invalid password was entered repeatedly.

**D**-Privileged Access Manager denied access to a resource, did not permit a login, or did not permit an update to the database because the accessor did not have sufficient authorization.

**E**-Serevu enabled a disabled user account.

**F**-An attempt to update the database failed.

**I**-Serevu disabled a user account.

**M**-The executed command started or shut down a daemon.

**O**-A user logged out.

**P**-Privileged Access Manager permitted access to a resource or permitted a login.

**S**-The database was successfully updated.

**T**-An audit record was written because all the actions of the user are being traced.

**U**-A Trusted program (setuid or setgid) was changed; therefore it is no longer Trusted.

**W**-Access to the resource violated the access rules for the resource. However, Privileged Access Manager allowed the access because warning mode is set in the resource.

– **Host(host-name)**

The host involved in a TCP/IP connection.

– **Object(resource-name)**

For the resource that the user is attempting to access.

– **Reason(reason-number)**

The reason that the audit record is triggered.

– **Service(service-name)**

The name of the service requested from the remote host, such as telnet, ftp, or port number.

– **Source Host(hostname)**

The name of the host that contributed the record to the consolidated audit.

– **Stage(stage-number)**

The stage at which access was granted or denied. (See the lists of stage codes in the *Reference Guide*.)

– **Terminalterminal-name)**

The terminal that is attempting access or administration.

– **Uid(uid-number)**

The uid of the user who is attempting access or administration.

– **User(username)**

Users attempting access or administration; username is a name or pattern.

**NOTE**

Although some variables are more likely to be specified as patterns, you can use a pattern for any variable—even for something like a stage number.

• **Refining with Further Lines**

To refine your specifications, you can filter by differing criteria at the same time. Simply add one include/exclude line after another. For example:

```
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*)
```

The example specifies all login attempts by users whose names begin with dbms and who are at terminals that do not have names beginning with console\_.

• **Specifying the Destination**

Use a line *above* your sequence of include and exclude lines to specify the destination for the audit records you are including. For example:

```
mail weekwatch
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*) .
```

The example specifies that the email address weekwatch receives a report on all login attempts by users whose names begin with dbms and who are at terminals that do not have names beginning with console\_.

This type of line appears in the format of the log route configuration file as:

```
routing-method destination
```

You can use any of the following methods:

– **mail *address***

To email the audit record; *address* is the destination address. If it is not in the form user@host, it is checked against local user lists and the NIS mail alias map.

**NOTE**

If address is a user name and surrogate requests to that user's account are audited, the audit records accumulate endlessly.

– **screen *username***

To display the audit record on the screen of the specified user, if that user is logged in at the current host when selogrd forwards the audit record. If the user is not logged in, the display is canceled, not postponed.

– **cons *hostname***

**NOTE**

To send the audit record to the Security Administrator GUI of the secmon utility on the specified host. If that host is not available, the display is terminated, not postponed.

- **file *textfilename*** To write the audit record in the specified ASCII file; *textfilename* must be an absolute path name and selogrd must have access to the file. Selogrd includes everything by default so you have to exclude everything and include what you want to be written to the file. For example:

```
LoginRule
file /data/audit_login_data.txt
include User(dbms*) Class(LOGIN) .
format filesize(10240000) .
.
```

– **host *hostname***

To send the audit record to the audit log collector on the specified host. If that host is not available, selogrd tries again later.

– **notify mail or notify default**

To email the audit record to the address that the audit record itself specifies.

– **notify screen**

To display the audit record on the screen of the user that the audit record itself specifies. If the user is not logged on, the display is canceled, not postponed.

– **syslog *priority***

To send the audit records to the syslog with a specified log priority:

- a. **LOG\_EMERG** System is unusable.
- b. **LOG\_ALERT** Action must be taken immediately.
- c. **LOG\_CRIT** Critical conditions
- d. **LOG\_ERR** Error conditions
- e. **LOG\_WARNING** Warning conditions
- f. **LOG\_NOTICE** Normal but significant condition

- g. **LOG\_INFO** Informational
- h. **LOG\_DEBUG** Debug-level messages

- **Proper Sequence for Lines**

It is important to arrange your include and exclude lines in proper sequence, properly delimited.

- Precede each sequence of lines (or single line) that you want to treat as a single complex filter with a title line. End it with a terminating line that consists of a single dot. Example:

```
dbms login from non-console
mail weekwatch
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*) .
.
```

The full sequence, including the title line and terminating line, is called a *section* of the file.

- If both include and exclude lines match the same audit record in the same section, the last match overrides all others.
- If no lines match a particular audit record, then the first line of the section is the deciding line for that record. If the first line is an include line, then the failure to match excludes the record. If the first line is an exclude line, then the failure to match includes the record for routing.
- If the section includes no include and exclude lines, then it includes all audit records for routing.

- **How Sections Coexist**

Whereas the lines of a section work together to produce a single decision whether a record is to be sent, different sections in the configuration file work independently. Whether an audit record is sent by one section, has no influence on whether the same audit record is sent by another section.

You can send the same selection of audit records to more than one destination, and the same destination can receive more than one selection of audit records.

In your configuration file, the total of all the include lines and exclude lines, from all the sections together, must not exceed 64 lines.

- **Including Comments**

To add a comment line to the configuration file, begin the line with a semicolon.

## Example 1

The following code is a sample configuration file, followed by its explanation.

```
; Product : CA ControlMinder
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----
Rule#1
mail jones@admhost
include      Class(*LOGIN*) Code(D) .
.
Rule#2
mail smith
include      Class(*SURROGATE*) Object(USER.root*) .
.
Rule#3
host venus
exclude      Class(UPDATE SU*) .
.
Rule#4
host venus
include      Class(*PROGRAM*) Object(/usr/bin/ps) .
```

The first five lines are comment lines.

The next four lines make up the first section, named Rule#1. They tell selogrd to mail a log record to the address jones@admhost whenever a login request is denied (code D reports denial):

```
Rule#1
mail jones@admhost
include      Class(*LOGIN*) Code(D) .
.
```

The next section is named Rule#2. It tells selogrd to mail a log record to the address smith whenever someone attempts to use the su command to enter the root account. The objects in the SURROGATE class are targets for the su command:

```
Rule#2
mail smith
include      Class(*SURROGATE*) Object(USER.root*) .
.
```

The next section is named Rule#3. It tells selogrd to send a log record to the collector on the host venus whenever someone attempts database administration, unless the class name begins with the letters SU (the matching classes are SURROGATE and SUDO):

```
Rule#3
host venus
exclude      Class(UPDATE SU*) .
```

The last section is named Rule#4. It tells selogrd to send a log record to the collector on the host venus whenever someone attempts to use the ps command:

```
(Code 1 8pt) Rule#4
host venus
include      Class(*PROGRAM*) Object(/usr/bin/ps) .
.
```

## Example 2

The following configuration file sends *all* audit records to the collector on the station named loghost:

```
; Product : CA ControlMinder
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----
Rule#1
host loghost
.
```

- Return Codes**

You can associate each type of record in the configuration file with one or more Privileged Access Manager return codes. (For a complete list of the return codes see the description of *code(return-code)* in Specifying Audit Records in this section.) The following table describes the record types and their associated return codes.

Record Type	Class or Event	Associated Return Codes
Login	LOGIN LOGINDISABLE LOGINENABLE	D, P, W I E

Logout	LOGOUT	O
TCP/IP	HOST	D, P
Resource classes	<i>Class name</i>	D, P, W
Watchdog	PROGRAM SECFILE	U U
Password administration	PWCHANGE	D
Down	SHUTDOWN	D, S
Start	START	S
Privileged Access Manager database administration	UPDATE	D, F, S

### Manage JCS Connector Log File Names and Log Levels

You can use the following configuration file to manage log file names for SSH, Network-device, Sybase, ACF2, and RACF JCS log file connectors.

```
<JCS-directory>\conf\log4j.properties
```

This file is used to set the log file names for each of the preceding connectors. The log file names are:

ssh.log

- network\_device.log
- sybase.log
- acf2.log
- racf.log

You can configure the log detail level for each connector according to the following level scale:

Trace

- Debug
- Info
- Warn
- Error
- Fatal

The SSH connector collects only logs from the level that is set on the scale and lower. For example, the SSH connector collects logs only from the debug, info, warn, error, and fatal levels when set as follows:

```
log4j.logger.com.ca.jcs.sshdyn=INFO, ssh
log4j.logger.com.ca.sesame.conn.unix=INFO, ssh
```

#### NOTE

Each connector log file is saved to a back-up and a new log is started each day.

### kbldaudit.cfg Filter Keyboard Logger Audit Records

#### Valid on UNIX

The **kbldaudit.cfg** file filters Keyboard Loggers (KBL) audit records. The file filters KBL audit records depending on the filter rule that you configure in the [INCLUDE] and [EXCLUDE] sections.

You can locate the file at */opt/CA/PAMSC/etc*.

- [INCLUDE]



The format of the [INCLUDE] section is as follows:

```
[INCLUDE]
LOGIN;<UserName>;<UserId>;<TerminalName>;<LoginProgram>;<AuthorizationResult>
TRACE;<TracedClassName>;<TracedObjectName>;<RealUserName>;<ACUserName>;<AuthorizationResult>;
```

When you add a filter rule to the [INCLUDE] section, the *kblaudit.cfg* file logs audit records that match the rule. The *kblaudit.cfg* file logs all the audit records when you fail to define a rule in the [INCLUDE] section.

In the [INCLUDE] section, ensure that you include the LOGIN rule. Without the LOGIN records, the *seaudit* utility fails to display session IDs. Without session IDs, the *kblaudit.cfg* file fails to log KBL audit records.

- **[EXCLUDE]**

The format of the [EXCLUDE] section is as follows:

```
[EXCLUDE]
TRACE;<TracedClassName>;<TracedObjectName>;<RealUserName>;<ACUserName>;<AuthorizationResult>;
```

When you add a filter rule to the [EXCLUDE] section, the *kblaudit.cfg* file logs audit records that do not match the rule. The *kblaudit.cfg* file logs all the audit records when you fail to define a rule in the [EXCLUDE] section.

### Example:

The following snippet of the *kblaudit.cfg* file excludes from the *kbl.audit* file the *usermod* operation events that the *test-user* performs.

```
[EXCLUDE]

TRACE;*;*;test-user;*;test-user;*;*;usermod*
```

The following snippet of the *kblaudit.cfg* file includes in the *kbl.audit* file the *cat* operation events that the *test-user* performs.

```
[INCLUDE]
LOGIN;*;*;*;*;*
TRACE;*;*;test-user;*;test-user;*;*;cat*
```

### NOTE

A \* in the rule syntax stands for any value.

## Login Rule Syntax

### Valid on UNIX

The Login rule filters keyboard loggers login events depending on the arguments that you specify. The format of the login rule is as follows:

```
LOGIN;<UserName>;<UserId>;<TerminalName>;<LoginProgram>;<AuthorizationResult>
```

- **<UserName>** Specifies the login name of the user to filter login events.
- **<UserId>**  
Specifies the login Id of the user to filter login events.
- **<TerminalName>**

Specifies the name of the local host that the user logs in.

- **<LoginProgram>** Specifies the name of the program that the user attempts to log in or log out.

**Limits:** cmdlog

- **<AuthorizationResult>** Specifies the authorization criteria to filter user login events.

**Limits:** P (permitted), D (denied), O (logout), \* (A wildcard that represents any value)

## Trace Rule Syntax

### Valid on UNIX

The Trace rule filters trace messages on user events depending on the arguments that you specify. The format of the trace rule is as follows:

```
TRACE;<TracedClassName>;<TracedObjectName>;<RealUserName>;<ACUserName>;<AuthorizationResult>;<TraceMessageMask>;<KBLSessionID>;<Optional><InputCommandName>;
```

- **<TracedClassName>**  
Specifies the name of the object class that the user tries to access.  
**Limits:** KBL raw, KBL output, KBL input, KBL execargs
- **<TracedObjectName>**  
Specifies the host that the user tries to access.
- **<RealUserName>**  
Specifies the name of the logged in user that generates trace records.
- **<ACUserName>**  
Specifies the name of the effective user who checks the rule. An effective user can be a logical user or a *setuid* user.
- **<AuthorizationResult>** Specifies the authorization criteria to filter trace messages.  
**Limits:** P (permitted), D (denied), \*
- **<TraceMessageMask>**  
Specifies the trace message mask criteria to filter trace messages.
- **<KBLSessionID>**  
Displays the keyboard logger sessions ID.
- **[Optional] <InputCommandName>** Specifies that the utility filters audit records based on the command a user executes on the host. The input command argument is optional.

## The lang.ini File

### Valid on UNIX

This section describes the tokens in the lang.ini file, used by the selang utility.

The lang.ini file contains the following sections:

- **general**  
Contains default parameters that apply to more than one type of resource; that is, both new resources and new users.
- **history**  
Contains default parameters for the selang history mechanism.
- **newres**  
Contains the default values that are assigned to the properties of new resource records. The default value is assigned unless you explicitly set a different value.
- **newusr**

Contains the default values that are assigned to the properties of new user records. The default value is assigned unless a different value is explicitly set.

- **properties**  
Contains tokens that specify values for user-defined properties, such as file locations for user-defined properties. The tokens have no default values; you must set them explicitly.
- **unix**  
Contains the default values that are assigned when a new user is defined to UNIX from within the selang command shell. The default value is assigned unless you explicitly set a different value.

## general

The [general] section contains default parameters that apply to more than one type of resource.

- **defaultOwner**  
The name of the owner assigned to a new record.  
If you do not specify a value, the creator of the new record is assigned as owner.

## history

The [history] section contains default parameters for the selang history mechanism.

- **HistFile**  
The name of the file where the commands in the history list are stored. The command list is loaded at the beginning of each session.  
No default value; that is, the history list is not saved at the end of a session.
- **HistSize**  
The number of commands (a positive integer between 10 and 100) stored by the history mechanism.  
**Default:** 30

## newres

The [newres] section contains default values that are assigned by the newres command. The newres command creates new resource records in the database. Each token in this section represents a newres parameter. Parameters not represented in the lang.ini file are assigned default values that are hard-coded in Privileged Access Manager. If you do not specify a value for a token, the default value specified in the table is applied.

- **DefaultAudit**  
The default audit mode for the new resource. Valid values are: none, all, success, failure.  
**Default:** failure
- **DefaultDay**  
The default day restrictions that apply to the resource. Valid values are: anyday, weekdays, mon, tue, wed, thu, fri, sat, sun.  
**Default:** anyday
- **DefaultNotify**  
The default email address to which alert messages regarding the resource record are sent.  
No default value; that is, no notification message is sent.
- **DefaultTime**  
The default time restrictions that apply to the resource. Valid values are: anytime, startTime:endTime.  
**Default:** anytime
- **DefaultWarning**  
Whether warning mode is enabled by default. Valid values are: yes, no.  
**Default:** no

## newusr

The [newusr] section contains the default values assigned by the newusr command, which creates new user records in the database. Each token in this section represents a newusr parameter. Parameters not represented in the lang.ini file are assigned default values that are hard-coded in Privileged Access Manager. If you do not specify a value for a token, the default value specified in the table is applied.

- **DefaultAudit**  
The default audit mode for the new user. Valid values are: none, all, success, failure, loginsuccess loginfailure.  
**Default:** failure loginfailure loginsuccess
- **DefaultDay**  
The default day restrictions that apply to the user when logging in to the system. Valid values are: anyday, weekdays, mon, tue, wed, thu, fri, sat, sun.  
**Default:** anyday
- **DefaultExpire**  
The default expiry date for the user record. Valid values are: expire[dd/mm/yy], expire-.  
**Default:** expire-
- **DefaultLocation**  
The default location in which the user works.  
No default value
- **DefaultNotify**  
The default email address to which alert messages are sent when the user logs in.  
No default value; that is, no notification message is sent.
- **DefaultOrg**  
The organization for which the user works.  
No default value
- **DefaultOrgUnit**  
The organizational unit in which the user works.  
No default value
- **DefaultTime**  
The default time restrictions that apply to the user when logging in to the system. Valid values are: anytime, startTime:endTime.  
**Default:** anytime

## properties

The [properties] section contains parameters that apply to user-defined properties.

- **UserDefinedTokensFile**  
The path for a definition file that contains context information for user-defined properties.  
**Default:** none
- **UserDefinedAttributesFile**  
The path for a definition file that contains attribute information for user-defined properties.  
**Default:** none

## User-Defined Properties

This section is complimentary to the sepropadm utility. It defines the selang context by which database properties created with sepropadm are recognized. Two definition files that use a format similar to the one used by sepropadm accomplish this. The location of these files is specified in the two tokens of this section.

**NOTE**

The properties must be defined in the database (using the sepropadm utility), before the definition files are loaded by selang. The definition files are loaded automatically when selang is run, during the initialization phase.

When these properties are defined in both the appropriate definition files and the database, you can use them in selang commands like any other Privileged Access Manager defined property.

**WARNING**

Do **not** use the sepropadm utility with a description file that was **not** certified by your vendor's support personnel.

**The Definition Files**

To get selang to recognize the new user-defined properties, selang loads two \*.def files during its initialization: the Tokens file and the Attributes file.

**The Tokens File****User Defined Tokens File**

A definition file supplied by your vendor's support personnel. The definition file has the following format:

Lines that begin with a semicolon (;) are comments and are not processed.

One line must begin with the hash symbol (#). This line must precede the description lines.

The description line must conform to the following format:

```
TOKEN=%s DOMAIN=%d CLASS=%d COMMAND=%d
```

The following is a sample definition tokens file:

```
; Sample Token Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; -----
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# token definition file ; Format is : TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=NOEMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=NOAGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=217
TOKEN=NOTERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
```

**The Attributes File****User Defined Attributes File**

A definition file supplied by your vendor's support personnel. The definition file has the following format:

Lines that begin with a semicolon (;) are comments and are not processed.

One line must begin with the hash symbol (#). This line must precede the description lines.

The description line must conform to the following format:

```
PROPERTY=%s TYPE=%d FLAGS=%x
```

The following is a sample definition attributes file:

```
; Sample Attributes Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; -----
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# attributes definition file ; Format is : PROPERTY=EMAIL TYPE=306 FLAGS=8000
PROPERTY=EMAIL TYPE=5 FLAGS=8000
PROPERTY=AGE TYPE=306 FLAGS=8000
PROPERTY=AGE TYPE=5 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=306 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=5 FLAGS=8000
```

### WARNING

Do **not** use `selang` with a definition file that was **not** certified by your vendor's support personnel.

## unix

The `[unix]` section contains the default values that are assigned by the `newusr` command when a user is added to UNIX. Each token in this section represents an argument of the `unix` parameter. UNIX arguments not represented in the `lang.ini` file are assigned default values that are hard-coded in Privileged Access Manager.

- **DefaultPGroup**  
The default group assigned to new users. If you specify a default shell in the server's `seos.ini` file, it overrides the value specified here.  
**Default:** `other`
- **DefaultShell**  
The default shell of new users. If you specify a default shell in the server's `seos.ini` file, it overrides the value specified here.  
**Default:** `/bin/sh`
- **DefaultHome**  
The default home directory of the system. If you specify a default shell in the server's `seos.ini` file, it overrides the value specified here. The user's home directory is a subdirectory of the specified system home directory. For example, if the system home directory is `/home`, the new user's home directory is `/home/userName`. If you specify a home directory prefix in the server's `seos.ini` file, it overrides the value specified here.  
For those familiar with earlier versions, the token `DefaultHome` replaces `HomeDirPrefix`.  
**Default:** `/home`

## The pmd.ini File

### Valid on UNIX

The `pmd.ini` file contains various setup and initialization settings Privileged Access Manager uses when building and maintaining a specific PMDB. It consists of several sections and each section contains multiple settings:

Section	Description
<code>endpoint_management</code>	Policy Model endpoint management settings.
<code>lang</code>	Privileged Access Manager management interface ( <code>selang</code> ) settings for working with a Policy Model.
<code>logmgr</code>	PMDB logging facility settings.
<code>passwd</code>	User and password data settings.
<code>pmd</code>	Policy Model daemon ( <code>sepmdd</code> ) settings.

seos	Generic PMDB settings.
------	------------------------

## endpoint\_management

The [endpoint\_management] section contains the parameters that define endpoint management settings for the Policy Model.

- **AutoSync**  
Specifies to automatically synchronize the DH with the Message Queue server.  
**Limits:** 0,1  
**Default:** 0 (disabled)
- **debug\_mode**  
Specifies if Privileged Access Manager writes debug messages to the endpoint\_management.log file in the DMS directory (1).  
**Limits :** 0,1  
**Default :** 0 (debugging is disabled)  
**Note:** The log file is located at *ACInstallDir/log/endpoint\_management.log*
- **deployment\_lifetime**  
Specifies the deployment lifetime in days. Older deployments are removed at 2 am. To disable deployment cleanup, set this value to 0.  
**Default:** 30 days
- **operation\_mode**  
Specifies whether central (DMS) endpoint management through the Privileged Access Manager Message Queue is enabled.  
**Limits:** 0,1  
**Default:** 1 (enabled)

## lang (pmd.ini)

The [lang] section contains the parameters used by the Privileged Access Manager language program (selang) when building and maintaining a PMDB.

- **pre\_user\_exit**  
Specifies the path of the exit program to be executed before Privileged Access Manager issues a language command to update the UNIX user database.
- **post\_user\_exit**  
Specifies the path of the exit program to be executed after Privileged Access Manager issues a language command to update the UNIX user database.
- **pre\_group\_exit**  
Specifies the path of the exit program to be executed before Privileged Access Manager issues a language command to update the UNIX groups database.
- **post\_group\_exit**  
Specifies the path of the exit program to be executed after Privileged Access Manager issues a language command to update the UNIX groups database.

## logmgr (pmd.ini)

The [logmgr] section contains the parameters used by the PMDB logging facility.

- **audit\_back**  
Specifies the name of the PMDB audit backup file.

**Default:** pmd\_audit.bak

- **audit\_log**  
Specifies the name of the PMDB audit log file.  
**Default:** pmd\_audit
- **audit\_group**  
Specifies the group that can read the PMDB audit files. If no group is specified, only root can read the audit files. Privileged Access Manager does not verify the value of this token, so if you enter an invalid group name, Privileged Access Manager does not assign any group permissions to the audit log files.  
To change the group ownership of an existing audit log file, do the following:
  - a. Use the selang command chgrp to set the group ownership of the files.
  - b. Change the UNIX permissions by entering:

```
chmod 640 /opt/CA/PAMSC/log/seos.audit
```

**Default:** none

- **audit\_size**  
Specifies the size of the PMDB audit log file, in KB. Do not specify a size less than 50 KB.  
**Default:** 50 KB
- **error\_back**  
Specifies the name of the PMDB error backup file.  
**Default:** pmd\_error.bak
- **error\_log**  
Specifies the name of the PMDB error log file.  
**Default:** pmd\_error
- **error\_group**  
Specifies the group that can read the PMDB error files. If no group is specified, only root can read the error files. Privileged Access Manager does not verify the value of this token, so if you enter an invalid group name, Privileged Access Manager does not assign any group permissions to the error log files.  
To change the group ownership of an existing error log file, do the following:
  - a. Use the selang command chgrp to set the group ownership of the files.
  - b. Change the UNIX permissions by entering:

```
chmod 640 /opt/CA/PAMSC/log/seos.error
```

**Default:** none

- **error\_size**  
Defines the maximum size, in KB, of the PMDB error log file (defined by error\_log).  
**Limits:** A minimum value of 50 KB.  
**Default:** 50
- **max\_log\_size**  
Specifies the size of the PMDB general log file in KB.  
**Default:** 50 KB
- **pmd\_log\_level**  
Determines the messages that are logged in the PMDB log file.  
Valid values include the following:
  - 0-Do not log any entries.
  - 1-List only error messages.
  - 2-List error and informational messages.**Default:** 2
- **use\_syslog**



Determines whether the policy model daemon should write syslog messages.

**Default:** yes

## passwd (pmd.ini)

The [passwd] section contains parameters for UIDs and GIDs.

- **AllowedGidRange**

Specifies reserved numbers.

The integers below the first number and above the second number are reserved GIDs, which Privileged Access Manager cannot update.

**NOTE**

If only one integer is specified, all integers between one and the specified integer are reserved GIDs. If you specify a number that is larger than the upper limit, the default upper limit is applied (30000). If you specify a negative number, the default lower limit is applied (1). The applied lower limit for any number is +1 of the specified lower limit. For example, if *AllowedGidRange* = 100, 3000, then 101 is treated as the lower limit.

**Limits:** -1 to 2147483647

**Default:** 100,30000

- **AllowedUidRange**

Specifies reserved numbers.

The integers below the first number and above the second number are reserved UIDs, which Privileged Access Manager cannot update.

**NOTE**

If only one integer is specified, all integers between one and the specified integer are reserved UIDs. The applied lower limit for any number is +1 of the specified lower limit. For example, if *AllowedGidRange* = 100, 3000, then 101 is treated as the lower limit.

**Limits:** -1 to 2147483647

**Default:** 100,30000

## pmd (pmd.ini)

The [pmd] section contains the attributes used by the sepmd daemon when building and maintaining a PMDB.

- **\_min\_retries\_**

Specifies the minimum number of attempts that sepmd should make to resend the next queued update to an unavailable subscriber. The sepmd loops through the list of subscribers for outstanding updates and increments the counter each time it cannot resend the update to an unavailable subscriber. The subscriber is marked unavailable after the minimum number of attempts specified in this token.

**Default:** 4

- **\_QD\_timeout\_**

Specifies the maximum time, in seconds, that the sepmd daemon waits while attempting to update a subscriber database during the first scan of its subscriber list. If the time elapses and the daemon does not succeed in updating a subscriber, it skips that particular subscriber and tries to update the remainder of the subscribers on its list. After completing the first scan of the subscriber list, sepmd then performs a second scan in which it attempts to update the subscribers it did not succeed in updating during the first scan. During the second scan, it tries to update a subscriber until the connect system call times out (approximately 90 seconds).

**Default:** 3

- **\_retry\_timeout\_**

Specifies the time, in minutes, to wait before trying to resend an update to an unavailable subscriber, after the minimum number of attempts specified in `_min_retries_` has been made. It marks the subscriber available after the number of minutes defined by this token elapses.

A subscriber is marked unavailable until:

- It is manually released.
- `sepmdd` is manually shutdown and restarted. The `sepmdd` is restarted if:
  - a. if a language facility attempts to connect to it.
  - b. if a parent PMDB wants to send an update.
  - c. the pull option is triggered by a subscriber. This optionally occurs when Privileged Access Manager starts on the subscriber.
- The pull option is triggered by the unavailable subscriber.

#### NOTE

Shutting down `sepmdd` too often is not desirable because it takes time to restart the daemon, which results in slowing the whole propagation process. Allowing it to be on all the time is also undesirable because there maybe some stability issues, but it is only a conjecture.

**Default:** 30

- **`_shutoff_time_`**

Specifies the time, in minutes of activities before `sepmdd` quits. If the token value is zero, `sepmdd` never quits.

**Default:** 0

- **`always_propagate`**

If this token is set to no, commands that failed to execute by the policy model are not propagated to the subscribers.

**Default:** none

- **`exclude_file`**

Specifies an exclude file.

The exclude file contains host names (one on each line) that should be excluded from receiving policy model updates.

**Default:** none

- **`exclude_localhost`**

Tells the `pmdb` to exclude the local host from receiving updates as a subscriber.

Possible values: yes, no.

**Default:** no

- **`exclude_method`**

Enables/disables the promote offset in update file when subscriber is excluded.

Values:

"pmdwaitdo not promote offset"

Otherwise "bypass"

**Default:** `pmdwait`

- **`filter`**

Specifies the name of the filter file.

- **`force_auto_truncate`**

Specifies whether Privileged Access Manager truncates the update file even if there are no subscribers to the Policy Model.

You can truncate the update file manually (`sepmdd -t`), and Privileged Access Manager also truncates the file automatically based on a separate configuration setting (`trigger_auto_truncate`) that defines the event that triggers automatic truncation.

**Note:** If all subscribers to the Policy Model are "Out of sync", the Policy Model effectively has no subscribers.

**Default:** Yes

- **`group_file_name`**

Specifies the name of the group file for a new UNIX group. `sepmdd` saves the group entry of the new UNIX group in this file.

**Default:** group

- **is\_maker\_checker**

Specifies whether to use Dual Control. The valid values for this token are yes and no.

If **yes** is selected, then the PMDB cannot be updated directly, but only through a transaction; and each transaction entered by one administrator must be processed by another administrator before the commands are implemented on the PMDB.

**Default:** no

- **password\_file\_name**

Specifies the name of the password file for new UNIX users. `sepmdd` stores the password entry of new UNIX users in this file.

**Default:** passwd

- **send\_unix\_env**

Indicates whether `sepmdd` sends the contents of Policy Model password files and group files.

If this token is set to **yes**, the `sepmdd -n` option sends the contents of the Policy Model password files and group files.

If this token is set to **no**, the `sepmdd -n` option does not send the contents of the policy model password files and group files.

**Default:** yes

- **synch\_uid**

Determines whether `sepmdd` attempts to synchronize UIDs between a Policy Model and its subscribers. The valid values for this token are yes and no.

If the token is **no**, `sepmdd` does not attempt to synchronize UIDs. Users are assigned the first available UID on each subscriber host.

If the token is **yes**, `sepmdd` attempts to synchronize UIDs. For example, if a new UNIX user is created on the PMDB with a UID of 1000, `sepmdd` transfers that UID to the subscribers. If UID 1000 is already in use on one of the subscribers, then the update on that subscriber fails.

`sepmdd` only tries to synchronize UIDs if the original command sent to the PMDB did not specify a UID for the user. If the original command did specify a UID, the specified UID is sent to all the subscribers.

**Default:** yes

- **TNG\_Environment**

Specifies whether the database is created with special TNG classes and resources.

Valid values are:

"0" to create the database without the special TNG classes

"1" to create the database with all the special TNG classes

**Default:** 0

- **transaction\_lib**

Specifies the path of the maker-checker policy.

**Default:** /opt/CA/eTrustAccessControl/policies/maker

- **trigger\_auto\_truncate**

Defines the size of the Policy Model update file, in megabytes, that triggers an automatic truncating of the update file.

If you use a value that is less than the lower limit, Privileged Access Manager uses the default value. If you use a value that is greater than the upper limit, Privileged Access Manager uses the upper limit value.

**Limits:** 1 - 2000 MB

**Default:** 1024 MB

- **update\_while\_processing**

Defines the frequency at which the Policy Model propagates commands to subscribers while it is processing incoming events.

The frequency is a factor of the `updates_in_chunk` setting, and determines how many commands the PMD processes before it sends the next subscriber in line one set of commands. For example, if you set this to 3 and `updates_in_chunk` is set to 10, the PMD will process 30 commands before it sends a set of commands (10) once to the next subscriber in line. A value of 0 means that the PMD does not propagate commands while processing incoming events.

**Default:** 1

- **updates\_in\_chunk**

Determines the maximum number of commands that the Policy Model sends to each of its subscribers in each cycle of a loop.

**Default:** 20

- **UseEncryption**

Specifies whether update information saved to the updates.dat file is encrypted.

**Default:** no

- **UseShadow**

Determines whether to use a shadow file when you reference the PMDB native environment.

**Default:** no

- **YpServerSecure**

Specifies the name of the password shadow file (a security file on an NIS server) that is used for building the NIS password map. This token is relevant only if you set UseShadow to yes.

**Default:** /etc/shadow

## seos (pmd.ini)

The token of the [seos] section, which contains the global settings that are used by Privileged Access Manager, is described in the following table.

- **parent\_pmd**

Defines a comma-separated list of policy model databases (PMDBs) from which this PMDB accepts updates. This PMDB rejects updates from any PMDB that is not specified in this list.

You can also specify a file path that contains a line-separated list of PMDBs.

Set this token to "\_NO\_MASTER\_" for this PMDB to accept updates from any PMDB.

If you do not set this token, this PMDB does not accept updates from any PMDB.

Each PMDB is specified in the following format: pmd\_name@hostname

For example:

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
```

```
parent_pmd = /opt/CA/PAMSC/parent_pmdbs_file
```

**Default:** Token is not set (PMDb does not accept updates from any PMDB).

## The seos.ini Initialization File

### Valid on UNIX

The seos.ini file contains various setup and initialization tokens that are used by Privileged Access Manager. Each token occupies a line in the file, in the following format:

```
token=value
```

The lines containing the tokens for a particular utility, daemon, or other facility of Privileged Access Manager are grouped in sections. Each section starts with a header line that gives the section name inside square brackets. Every token belongs to a section. For example, the following line starts the section that governs the serevu utility:

```
[serevu]
```

The seos.ini file, as installed, is protected by Privileged Access Manager and cannot be updated while Privileged Access Manager is running. The file, as defined by default in Privileged Access Manager, has READ access because many utilities access this file during their processing. If they cannot read the seos.ini file, they fail.

Enter the following selang command to let an authorized user update the file while Privileged Access Manager is running:

```
newres FILE /opt/CA/PAMSC/seos.ini owner(authUser)
```

where *authUser* is the name of an authorized user. This command establishes that *authUser* is the owner of the file, and as the owner of the file, *authUser* can always update it.

You can use Privileged Access Manager Endpoint Management or the seini utility to read, add, modify, and delete tokens in initialization files.

#### NOTE

The seini utility can only update the seos.ini file when seosd is *not* running, or when a rule in the database specifically permits it.

Using the *secons -r* command, you can reload an seos.ini file with updated tokens without having to restart the seosd daemon.

The following table lists all the sections in the seos.ini file.

Section	Description
crypto	Cryptographic module library settings.
daemons	A list of Privileged Access Manager daemons the seload utility runs automatically.
Dependency	A list of products that use Privileged Access Manager as an embedded component, as defined by users.
devcalc	Policy deviation calculator (devcalc) settings.
kblaudit	Keyboard logging session tracking settings.
lang	Privileged Access Manager management interface (selang) settings.
ldap	LDAP server settings for the LDAP sample exit.
logmgr	Logging facility settings.
message	Message file settings.
mfsd	Mainframe synchronization daemon (mfsd) settings.
OS_user	Enterprise user store usage settings.
package	A list of installed Privileged Access Manager packages.
pam_seos	Pluggable Authentication Module (PAM) programming interface settings.
passwd	Password replacement and user-related services settings.
pmd	Common Policy Model database settings.
policyfetcher	Policy fetcher daemon (policyfetcher) settings.
seagent	seagent daemon settings.
segrace	User login information utility (segrace) settings.
seini	Configuration file management utility (seini) attributes.

selock	Desktop inactivity protection utility (selock) settings.
selogrd	Log routing daemons (selogrd and selogrcd) settings.
seos	Global configuration settings.
SEOS_syscall	SEOS_syscall kernel module settings.
seosd	Authorization daemon (seosd) settings.
seosdb	Database checking and rebuilding settings.
seoswd	Watchdog daemon (seoswd) settings.
serevu	Unsuccessful login attempts resolution utility (serevu) utility settings.
sesu	Privileged Access Manager switch user utility (sesu) settings.
sesudo	Privileged Access Manager substitute user do utility (sesudo) utility settings.
standalone	Standalone computer administration settings.
strong_auth	Strong authentication server settings.
tcp_communication	Common TCP connection settings.

## crypto

In the [crypto] section, the tokens control aspects associated with the cryptography module.

- **ca\_certificate**  
Defines the full pathname to the Certificate Authority (CA) certificate database.  
**Default:** *ACInstallDir/data/crypto/def\_root.pem*
- **communication\_mode**  
Specifies whether secure socket layer (SSL) protocols are enabled.  
If you set this token to *ssl\_only*, only SSL V2, SSL V3, and TLS connections are enabled. This means that this computer cannot communicate with computers that do not support SSL, and so cannot communicate with computers that are running versions of Privileged Access Manager earlier than r12.0, which do not support SSL.  
**Note:** Computers that are running Privileged Access Manager r12.0 and later do support SSL.  
If the *fips\_only* token is set to 1, the actual communication mode is set to *ssl\_only* in FIPS mode (TLS), and the *communication\_mode* token is ignored.  
Valid values are:
  - *all\_modes*
  - *ssl\_only*
  - *non\_ssl***Default:** *non\_ssl*
- **CAPKIHOM**  
Defines the installation directory of CAPKI.  
**Default:** */opt/CA/SharedComponents/CAPKI*
- **encryption\_methods**  
Specifies the encryption libraries that the Privileged Access Manager Agent uses to decrypt messages. The Agent attempts to use each library in the list, in turn, until the decryption is successful.  
**Limits:** *libaes256, libaes192, libaes128, libdes, libtripleDES, libscramble*  
**Default:** *libaes256, libaes192, libaes128, libdes, libtripleDES*
- **fips\_only**  
This token controls whether Privileged Access Manager works in FIPS only mode. In this mode, all non-FIPS functions are disabled.  
Valid values:

**1** Privileged Access Manager works in FIPS only mode

**0** Privileged Access Manager works in non-FIPS mode

**Default:** 0

- **LIBRARY\_PATH**

Defines the directory for the ETPKI cryptographic library.

- **private\_key**

Defines the full pathname to the subject private key.

**Default:** *ACInstallDir/data/crypto/sub.key*

- **sha\_mode** Defines the hashing mode of the sha signatures.

Values are: sha1, sha256, sha384, sha512

**Default:** sha512

- **ssl\_port**

Defines the port for SSL communications between Privileged Access Manager clients and services.

**Default:** 5249

- **subject\_certificate**

Defines the full pathname to the subject certificate.

**Default:** *ACInstallDir/data/crypto/sub.pem*

## daemons

In the [daemons] section, each token specifies whether (and if so, how) the seload utility executes a particular program from the Privileged Access Manager installation directory. Each token name corresponds to either a Privileged Access Manager daemon name or is a program nickname and can be assigned several values.

- *program-name*

Specifies one of two possibilities:

- The name of a daemon or other program to be matched with:
  - a *yes* value, so that seload runs the program with default parameters
  - a *no* value, so that seload does not run the program
  - a set of parameters, so that seload runs the program with those parameters

For example, enter the following to run serevu from the Privileged Access Manager installation directory with default parameters:

```
serevu=yes
```

Enter the following to refrain from running serevu; this is the same as using no serevu token

```
serevu=noEnter the following to run serevu from the CA ControlMinder installation directory
```

```
serevu=-f 3 -d 6m -t 1m -
```

s 5mA dummy string, to be matched with the absolute path name of a daemon or other program, f  
opt/CA/PAMSC/bin directory, with the specified parameters:

```
run_it=/opt/CA/PAMSC/bin/serevu -f 3 -d 6m -
```

t 1mTo include specifications for several programs, use the token once for each program.

serevu=yes

Enter the following to refrain from running serevu; this is the same as using no serevu token at all.

**Default:** no

#### NOTE

You do not need to specify the seosd daemon. seload always ensures that the seosd daemon is running.

- **seload\_wait\_timeout**

Specifies the time (in seconds) that seload waits until the main process is running.

**Default:** 45

## Dependency

In the [Dependency] section, each user-defined token specifies a product that uses Privileged Access Manager as an embedded component.

- *product-name*

Specifies a product that uses Privileged Access Manager as an embedded component. Valid values are:

**0** - Not an embedded product

**1** - An embedded product

**Default:** No default products specified

## devcalc

In the [devcalc] section, the tokens control aspects associated with the policy deviation calculator.

- **dms\_command\_retry\_interval**

Defines the number of seconds between each DMS notification command retry.

**Default:** 60

- **init\_ac\_db**

Obsolete.

- **max\_dms\_command\_retry**

Defines the maximum number of times the policy deviation calculator retries to send update notifications to the DMS before giving up.

**Default:** 3

- **max\_lines\_request**

Defines the maximum number of lines (from the policy deviation data file) that the *get devcalc* selang command returns at any one time. You then need to retrieve additional lines using the following command:

```
get devcalc params("offset=X")
```

XDefines the line offset returned by the previous *get devcalc* output.

```
get devcalc params("offset=X")
```

– X

Defines the line offset returned by the previous *get devcalc* output.

**Default:** 50

## kblaudit

The tokens in the [kblaudit] section control the behavior of the Keyboard Logger session tracking program.

- **audit\_back**

Specifies the name of the Keyboard Logger backup audit log file.

**Default:** *ACInstallDir/log/kbl.audit.bak*

- **audit\_group**



Specifies the group that can read the audit logs. If you set this token to **none**, only root can read the audit logs. This token does not verify the value of this token. If you enter an invalid group name, the token does not assign any group permissions to the audit log files.

To change the group ownership of an existing audit log file, complete the following steps:

Use the `selang` command `chgrp` to set the group ownership of the files.

Change the UNIX permissions by entering the following command:

```
chmod 640 ACInstallDir/log/seos.audit
```

**Default:** none

- **audit\_log**

Specifies the name of the Keyboard Logger audit log file.

**Default:** *ACInstallDir/log/kbl.audit*

- **audit\_max\_files**

Specifies the maximum number of audit log files to keep in backup mode. When reached, deletes the earliest backup file when the latest file is created.

**Limits:** a positive integer.

**Default:** 0

**NOTE**

When set to 0, accumulates backup files and does not delete earlier files.

- **audit\_size**

Specifies the maximum size, in KB, of the audit log file.

**Minimum value:** 50 KB

**Default:** 24000

**Note:** stops writing audit records to the audit file when the audit file size exceeds 2 GB.

- **BackUp\_Date**

Specifies the criterion by which the session backs up the audit log file, and if it adds a timestamp to the backup file name.

*Always* backs up the audit log file when it reaches the size that is specified in the `audit_size` configuration setting.

**Values:** none, yes, daily, weekly, monthly

- **yes:** The session backs up the audit log file when it reaches the size that is specified in `audit_size`. The session adds a timestamp to the backup file name.
- **none:** The session backs up the audit log file when it reaches the size that is specified in `audit_size`. The session does not add a timestamp to the backup file name.
- **daily, weekly, monthly:** The session backs up the audit log file whenever the specified interval has elapsed *and* when it reaches the size that is specified in `audit_size`. The session adds a timestamp to the backup file name. However, if no audit events are written to the audit log file in the specified interval, the session does not back up the file after the interval elapses.

**Note:** Counts the specified interval from the time that it creates the first audit log file, and backs up the file at midnight on the appropriate day.

**Example:** The configuration setting has a value of `weekly`, and creates the audit log file at 9:00 am on Friday April 1. Many audit events occur this week and the audit log file exceeds the `audit_size` configuration setting on Monday 4 April. backs up the audit log file on 4 April and adds a timestamp to the backup file name. A week after the audit log file was first created, at midnight Friday 8 April, again backs up the audit log file and adds a timestamp to the backup file name.

**Default:** NONE

- **cmd\_log**

Specifies the link to the Keyboard Logger `cmdlog` binary file.

**Default:** */etc/AC*

- **debug\_backup\_dir**

Specifies the location of the backup debug messages files.

**Default:** /opt/CA/PAMSC/log/kbl\_debug

- **debug\_backup\_num**

Specifies the number of debug files to backup.

**Default:** 2

- **debug\_file**

Specifies the location of the file that stores the Keyboard Logger debug messages.

**Default:** /opt/CA/PAMSC/log/kbl\_debug/cmdlog

- **debug\_level** Specifies the minimal level of debug messages to save.

**Values:**

- disabled: Messages are not saved
- critical: CRITICAL messages are saved, only
- very\_high: CRITICAL + VERY\_HIGH
- high: CRITICAL + VERY\_HIGH + HIGH
- normal: CRITICAL + VERY\_HIGH + HIGH + NORMAL
- low: CRITICAL + VERY\_HIGH + HIGH + NORMAL + LOW

**Default:** critical

- **debug\_size**

Specifies the maximum size (MB) of the debug messages file.

**Default:** 256 MB

- **error\_back**

Specifies the name of the Keyboard Logger error log backup file.

**Default:** *ACInstallDir*/log/kbl.error.bak

- **error\_group**

Specifies the group that can read the error log files. If you set this token to **none**, only root can read the error log files. Does not verify the value of this token, so if you enter an invalid group name, does not assign any group permissions to the error log files.

To change the group ownership of an existing error log file, complete the following steps:

Use the selang command `chgrp` to set the group ownership of the files.

Change the UNIX permissions by entering the following command:

```
chmod 640 ACInstallDir/log/seos.audit
```

**Default:** none

- **error\_log**

Specifies the name of the Keyboard Logger error log file.

**Default:** *ACInstallDir*/log/kbl.error

- **error\_size**

Defines the maximum size, in KB, of the error log file.

**Limits:** A minimum value of 50 KB

**Default:** 500

- **kbl\_enabled**

Specifies whether the Keyboard Logger is enabled.

**Values:** yes, no

**Default:** no

- **kbl\_flush\_timeout**

Specifies the user session inactivity interval, in seconds, after which the printable logged data is stored in the kbl audit file. Set the token to 0 to disable.

**Default:** 30

- **kbl\_output\_limit**

Specifies the limit (bytes) for storing the output that is collected after the last user input.

**Default:** 0 (no limit)

- **Kbl\_seos\_trace**  
Specifies whether seosd activates trace on session and sends user activity data to the Keyboard Logger.  
**Values:** yes, no  
**Default:** yes
- **kbl\_trace**  
Specifies whether to print the Keyboard Logger debug messages.  
**Values:** 0 (no tracing), 1 (use tracing)  
**Default:** 0
- **OS\_etc\_shells**  
Specifies the name of the operating system shells file.  
**Default:** /etc/shells
- **socket\_name**  
Specifies the socket name for the Keyboard Logger audit manager.  
**Default:** *ACInstallDir*/kblserver

## lang

In the [lang] section, the tokens specify the attributes used by the selang command language programs: selang, Security Administrator, and seadm.

- **check\_password**  
Determines whether selang requests users to specify their own passwords. Valid values include:  
**no**-selang does not require any passwords  
**yes**-Users are prompted to enter their passwords.  
**Default:** no
- **exit\_timeout**  
Specifies the maximum time, in seconds, that allows the exit program to execute. After this time has passed, the token kills the exit program.  
**Default:** 30
- **exits\_dir**  
Specifies the target directory where exits are installed by the *ACInstallDir*/bin/install\_exits.sh shell script.  
**Default:** *ACInstallDir*/exits
- **exits\_source\_dir**  
Specifies the source directory of the exits to be installed by the *ACInstallDir*/install\_exits.sh shell script.  
**Default:** *ACInstallDir*/samples/exits-src
- **help\_path**  
Specifies the directory in which lang help files are located.  
**Default:** *ACInstallDir*/data/langhelp
- **HNODE\_max\_events**  
Specifies the maximum number of health status events that the HNODE record writes. If events exceed the configured maximum number, then the oldest events are removed.  
**Default:** 10
- **language**  
Defines the language Privileged Access Manager installs in (for internal use).  
**Default:** english
- **max\_groups\_buffsize**  
Specifies the buffer size, in KB, that the security administrator uses when communicating with the database. This token is used when a UNIX update needs to be applied.  
**Default:** 128
- **no\_check\_password\_users**

Specifies users who are not asked to enter their passwords.

This token is relevant only if the token check\_password is set to **yes**.

Valid values include a list of users separated by commas.

**Default:** none

- **passwd\_copy**

Specifies how the password file (/etc/passwd) or PMDB password file (/PMDB\_Directory/policies/pmdb/passwd) is updated when you copy the temporary file back to the original after changing user information. Valid values include:

**fast\_copy** - Copies information over the file.

**rename** - Changes the directory to point to the new file.

**Default:** fast\_copy

- **post\_group\_exit**

Specifies the path of the exit program to be called after a group command is executed in the UNIX environment.

**Default:** ACInstallDir/exits/lang\_exit.sh

- **post\_user\_exit**

Specifies the path of the exit program to be called after a user command is executed in the UNIX environment.

**Default:** ACInstallDir/exits/lang\_exit.sh

- **pre\_group\_exit**

Specifies the path of the exit program to be called before a group command is executed in the UNIX environment.

**Default:** ACInstallDir/exits/lang\_exit.sh

- **pre\_user\_exit**

Specifies the path of the exit program to be called before a user command is executed in the UNIX environment.

**Default:** ACInstallDir/exits/lang\_exit.sh

- **query\_size**

Specifies the maximum number of records to be listed in a database query.

**Default:** 100

- **RecvTimeOut**

Specifies the maximum time, in seconds, that selang waits to receive information before timing out.

If you set the value to 0, there is no time-out.

**Default:** 60

- **SendTimeOut**

Specifies the maximum time, in seconds, that selang waits to send information before timing out.

If you set the value to 0, there is no time-out.

**Default:** 60

- **SetBlockRun**

Specifies whether to check if a program is trusted and block the execution of untrusted programs. The execution blocking is performed regardless whether the program is a setuid or a regular program.

Valid values include the following:

**yes**-All programs that are defined with viapgm authorization rules have the blockrun property set to yes.

**no**-All programs that are defined with viapgm authorization rules have the blockrun property set to no.

**suid**-All setuid programs have the blockrun property set to yes, and all other programs have the blockrun property set to no.

**Default:** yes

- **swap\_deletion\_order**

Defines the order in which the "ru *userName* unix" command (user deletion) is executed in selang. Typically, this command is first executed in the AC environment, and then in the UNIX environment. Sometimes (for example, a group administrator deleting a user) where you would want to reverse this order.

Valid values are:

**no** - remove the user from the AC environment before the UNIX environment.

**yes** - remove the user from the UNIX environment before the AC environment.

**Default:** no

- **timeout**

Specifies the maximum time, in seconds, the client waits for seosd daemon to respond. If seosd does not respond within this period, an error message is sent noting that seosd is not responding. The client then stops trying to connect to seosd.

**Default:** 90

- **use\_old\_commands**

Specifies whether to disable old ACF2 compatibility commands (ag, lg, rg, lu, au, and so on).

**Limits:** 0do not support old commands, 1support old commands

**Default:** 1 (support old commands)

- **use\_unix\_file\_owner**

Specifies whether a UNIX owner of a file can define the file. If the value is yes, an owner of a file in UNIX can define it using the newres or newfile command.

If the file is already defined, the user cannot change its parameters in the database unless the user is allowed to do so according to the normal authorization rules.

Valid values are yes and no.

**Default:** no

## ldap

In the [ldap] section, the tokens specify the attributes that are used to locate the LDAP server and input data. These parameters are used only by the ldap sample exit located in *ACInstallDir/samples/ldap/exits/S50CREATE\_Ldap\_u.sh*.

- **base\_entry**

Specifies the point in the LDAP directory tree to be used as the base entry point.

For example, you can use *o=organization\_name, c=country\_name*.

**Default:** Token not set

- **host**

Specifies the host name of the LDAP server.

**Default:** Token not set (localhost)

- **path**

Specifies the LDAP client base directory.

**Default:** Token not set (/usr/local/ldap)

- **port**

Specifies the LDAP server port (optional)

**Default:** Token not set (389)

## logmgr

In the [logmgr] section, the tokens control the behavior of the logging facility.

- **audit\_back**

Specifies the name of the audit log backup file. Only Privileged Access Manager can write to this file. Users can have READ access only to this file.

**Default:** *ACInstallDir/log/seos.audit.bak*

- **audit\_group**

Specifies the group that can read the audit logs. If you set this token to **none**, only root can read the audit logs.

Privileged Access Manager does not verify the value of this token. If you enter an invalid group name, the product does not assign any group permissions to the audit log files.

To change the group ownership of an existing audit log file, complete the following steps:

Use the selang command *chgrp* to set the group ownership of the files.

Change the UNIX permissions by entering the following command:

```
chmod 640 ACInstallDir/log/seos.audit
```

**Default:** none

- **audit\_log**

Specifies the name of the audit log file. When this file reaches the size that is specified in *audit\_size*, Privileged Access Manager does the following actions:

- Closes the file
- Renames it with the name in *audit\_back*
- Creates an audit log. Only Privileged Access Manager can write to this file. Users can have READ access only to this file.

**Default:** *ACInstallDir/log/seos.audit*

- **audit\_max\_files**

Defines the maximal number of audit log backup files accumulates when it performs date-triggered backups. When the BackUp\_Date configuration setting is set to anything other than *none*, continuously accumulates date-triggered backup files. This configuration setting lets you reduce disk space uses for audit log backups. When the number of audit log backup files reaches the limit that you set, Privileged Access Manager deletes the oldest backup file when it creates the newest.

**Values:**

- **0** keep all audit log backup files.
  - a. *na* positive integer greater than zero.

**Note:** You cannot remove redundant audit log backup files manually because Privileged Access Manager protects these files automatically. Also, if the audit reporting is enabled, Privileged Access Manager does not delete a backup file until the Report Agent finishes processing it.

**Default:** 0

- **audit\_size**

Specifies the maximum size, in KB, of the audit log file.

Minimum value: 50 KB

**Default:** 10240

**NOTE**

stops writing audit records to the audit file when the audit file size exceeds 2 GB.

- **BackUp\_Date**

Specifies the criterion by which Privileged Access Manager backs up the audit log file, and if it adds a timestamp to the backup file name.

*always* backs up the audit log file when it reaches the size specified in the *audit\_size* configuration setting.

**Values:** none, yes, daily, weekly, monthly

- **yes:** backs up the audit log file when it reaches the size that is specified in *audit\_size* and adds a timestamp to the backup file name.
- **none:** backs up the audit log file when it reaches the size that is specified in *audit\_size* and does not add a timestamp to the backup file name.
- **daily, weekly, monthly:** backs up the audit log file whenever the specified interval has elapsed *and* when it reaches the size that is specified in *audit\_size*, and adds a timestamp to the backup file name. However, if no audit events are written to the audit log file in the specified interval, Privileged Access Manager does not back up the file after the interval elapses.

**Note:** counts the specified interval from the time that it creates the first audit log file, and backs up the file at midnight on the appropriate day.

**Example:** The configuration setting has a value of weekly and Privileged Access Manager creates the audit log file at 9:00 a.m. Friday 1 April. Many audit events occur this week and the audit log file exceeds the *audit\_size* configuration setting on Monday 4 April. Privileged Access Manager backs up the audit log file on 4 April and adds a timestamp to the backup file name. A week after the audit log file was first created, at midnight Friday 8 April, the product again backs up the audit log file and adds a timestamp to the backup file name.

**Default:** NONE

- **error\_back**

Specifies the name of the error log backup file.

**Default:** *ACInstallDir/log/seos.error.bak*

- **error\_group**

Specifies the group that can read the error log files. If you set this token to **none**, only root can read the error log files. The product does not verify the value of this token. If you enter an invalid group name, the product does not assign any group permissions to the error log files.

To change the group ownership of an existing error log file, complete the following steps:

Use the `selang` command `chgrp` to set the group ownership of the files.

Change the UNIX permissions by entering the following command:

```
chmod 640 ACInstallDir/log/seos.audit
```

**Default:** none

- **error\_log**

Specifies the name of the error log file. When this file reaches the size that is specified in *error\_size*, Privileged Access Manager does the following actions:

- Closes the file
- Renames it with the name in *error\_back*
- Creates an error log. Only Privileged Access Manager can write to this file.

**Default:** *ACInstallDir/log/seos.error*

- **error\_size**

Defines the maximum size, in KB, of the error log file.

**Limits:** A minimum value of 50 KB.

**Default:** 50

- **irecorder\_audit**

Specifies whether the IR API library routes audit events of existing PMDs in addition to the local security daemon audit events.

all - routes audit events of Policy Models in addition to the local security daemon audit events.

localhost - routes audit events of the local security daemon only.

**Default:** all

- **logconnected**

Prevents TCP-CONNECTED records from being written to the audit log.

Set `logconnected` to No to use this feature.

**Default:** no

## message

In the [message] section, the tokens control the behavior of the message utility `semsgtool`.

- **dashboard\_messages** Indicates if the installation status was sent to the server for monitoring.

**Values:** Yes, No

**Default:** No

- **filename**

Specifies the location and name of the file that supplies most of the messages that appear in response to typed `selang` commands.

**Default:** *ACInstallDir/data/seos.msg*

- **MessagesDirectory**

Specifies the location of the messages file.

**Default:** *ACInstallDir/data/msg*

## mfsd

In the [mfsd] section, the tokens define the mainframe synchronization daemon options.

- **mfsd\_trace\_file**

Specifies the location of the file to which the mainframe synchronization daemon mfsd trace messages are written. If this token is set to **no**, the trace file is not created.

**Default:** *ACInstallDir/log/mfsd.trace*

## **OS\_user (seos.ini)**

The tokens in the [OS\_User] section define the settings used by Privileged Access Manager for enterprise users and enterprise groups.

- **create\_user\_in\_db**

Specifies whether creates an XUSER record for a user who is not defined to, when that user logs in.

Note: This setting applies only if you use enterprise users (osuser\_enabled is set to 1).

**Limits:** yes, no

**Default:** yes

- **nonunix\_unabgroup\_enabled**

Specifies whether supports non-UNIX groups of users in the UNAB database.

**Limits:** yes, no

**Default:** no

- **nonunix\_ldapgroup\_enabled**

Specifies whether supports non-UNIX groups of users, on LDAP servers.

**Limits:** yes, no

**Default:** no

- **osuser\_enabled**

Specifies whether enterprise users and groups are enabled.

**Limits:** yes, no

**Default:** yes

- **UserCache\_groups\_max**

Defines the maximum number of groups in the runtime user cache table.

**Default:** 1000

- **UserCache\_max**

Defines the maximum number of entries in the runtime user cache table.

**Default:** 20000

- **UserCache\_timeout**

Defines the interval (in minutes) before a record is removed from the runtime user cache table.

**Default:** 60

- **verify\_osuser**

Specifies whether verifies that a user exists in an enterprise store before it creates an enterprise user record (XUSER) in.

**Limits:** No - Lets you create an enterprise user record only if that user is defined in the enterprise user store. Yes - Always lets you create an enterprise user record.

**Default:** no

## **package**

In the [package] section, the tokens specify the packages you selected to install.

- **Client, Server, Admin, Mfsd, Tng, Stop, Api**

Indicates whether you selected to install the specified package.

**Default:** no



## pam\_seos

### NOTE

In the [pam\_seos] section, the tokens help you to more fully exploit the programming interface PAM (Pluggable Authentication Module).

- **api\_update\_lastacctest**  
Specifies whether the API libraries update the last access time and date of a user (through SEOS\_VerifyCreate).  
Valid values are:  
**0** - the last access time and date is not updated.  
**1** - the last access time and date is updated.  
**Default:** 0
- **bypass\_services**  
Defines which services PAM bypasses.  
**Default:** ftp, vsftpd
- **call\_segrace**  
Specifies whether to call the segrace utility with any login automatically.  
Valid values are yes and no.  
**Default:** no
- **call\_sepass**  
Specifies whether to use the sepass utility in the pam\_seos password management service.  
**Values:** No, Yes  
**Default:** No
- **debug\_mode\_for\_user**  
Specifies whether to inform the user of the reason for the login denial.  
Valid values are yes and no.  
**Default:** no
- **failed\_login\_file**  
Specifies the location of the failed login audit file pam\_seos.  
**Default:** *ACInstallDir/pam\_seos\_failed\_logins.log*
- **pam\_login\_events\_enabled**  
Specifies whether pam\_seos sends login events to seosd.  
**Values:** **0** - do not send login events; **1** - send login events  
**Default:** 1
- **pam\_get\_groups**  
Specifies whether pam\_seos retrieves user groups from operating system.  
**Values:** **0** - do not attempt to retrieve groups; **1** - attempt to retrieve groups  
**Default:** 1
- **pam\_groups\_timeout**  
Defines the timeout interval, in seconds, that Privileged Access Manager PAM uses for API to retrieve user groups.  
**Default:** 10
- **PamPassUserInfo**  
Specifies whether pam\_seos sends user information to seosd. This token is required when you use enterprise users, which Privileged Access Manager has no information for. Set this setting to 0 if you are not using enterprise users (osuser\_enabled = no).  
**Values:** **0** - do not send user information; **1** - send user information.  
**Default:** 1
- **pam\_surrogate\_events\_enabled**  
Specifies whether pam\_seos sends surrogate events to seosd.  
**Values:** **0** - do not send surrogate events; **1** - send surrogate events.  
**Default:** 1
- **process\_failed\_logins**

Specifies whether pam\_seos calls pam\_authenticate to authenticate user passwords and process failed logins.

Set this token to 0 if you do *not* want pam\_authenticate to be called twice.

**Values:** **0** - do not call pam\_authenticate from the Privileged Access Manager PAM module; **1** - call pam\_authenticate from the Privileged Access Manager PAM module.

**Default:** 1

- **serevu\_use\_pam\_seos**

Specifies whether serevu uses the pam\_seos login failure log file instead of the system file.

This feature increases the accuracy of serevu.

**Default:** yes

## passwd

In the [passwd] section, the tokens define password replacement and other user-related services.

- **AllowedGidRange**

Specifies the range of GIDs that the user can add, update, and delete. Values outside this range represent reserved GIDs that Privileged Access Manager cannot update.

**NOTE**

If only one integer is specified, all integers between the specified integer and the default upper limit (30000) are reserved GIDs. If you specify a number that is higher than the upper limit, the default upper limit is applied. If you specify a negative number that is less than the lower limit, the default lower limit (100) is applied. The applied lower limit for any number is +1 of the specified lower limit. The applied higher limit for any number is -1 of the specified higher limit. For example, if *AllowedUidRange* = 100, 3000, then 101 is treated as the lower limit and 2999 is treated as the higher limit.

**Limits:** -1 to 2147483647

**Default:** 100,30000

- **AllowedUidRange**

Specifies the range of UIDs that the user can add, update, and delete. Values outside this range represent reserved UIDs that Privileged Access Manager cannot update.

**NOTE**

If only one integer is specified, all integers between the specified integer and the default upper limit (30000) are reserved UIDs. If you specify a number that is higher than the upper limit, the default upper limit is applied. If you specify a negative number that is less than the lower limit, the default lower limit (100) is applied. The applied lower limit for any number is +1 of the specified lower limit. The applied higher limit for any number is -1 of the specified higher limit. For example, if *AllowedUidRange* = 100, 3000, then 101 is treated as the lower limit and 2999 is treated as the higher limit.

**Limits:** -1 to 2147483647

**Default:** 100,30000

- **AllowRootProp**

Specifies whether root password changes made using sepass -p or sepass -s are sent to the Policy Model. The PMD then propagates the password to its subscribers.

Valid values are yes and no.

**Default:** no

- **change\_pam**

Specifies whether the local host uses PAM for password authentication and changes in the LDAP database.

**Default:** no

- **Check\_Adm\_Rules**

Specifies whether to enforce password rules for ADMIN and PWMANAGER users.

**Default:** no

- **Check\_All\_User\_Rules**

Specifies whether `selang` checks the Password Rules for all the users.

Valid values are `yes` and `no`.

If this token is set to `yes`, `selang` checks the Password Rules for all the users.

If this token is set to `no`, `selang` checks the Password Rules only for the user who changes the password.

**Default:** `no`

#### NOTE

This token is supported when using the API only.

- **CreateHashedPasswdDatabase**

(DEC UNIX only). Specifies whether an exit script runs after each Privileged Access Manager command that creates, updates, or removes a user record, or after each user password changed with the `sepass` utility.

#### NOTE

For more usage instructions, see the README file in `ACInstallDir/samples/exits-src/USER_POST` directory.

**Default:** `no`

- **DefaultHome**

Specifies the default home directory of the system. The home directory of the user is a subdirectory of the specified system home directory. For example, if the system home directory is `/home`, the new home directory of the user is `/home/username`. If specified, the value for this token overrides the value in the client `lang.ini` file. If you specify `nohomedir`, then a home directory is not automatically set.

**Default:** `/home`

- **DefaultPasswdCmd**

Specifies the default password program. If specified, this password program is used when `sepass` is started and `seosd` is not running.

**Default:** `/bin/passwd`

- **DefaultPgroup**

Specifies the primary group that Privileged Access Manager assigns to a new UNIX user if no value is entered.

**Default:** `other`

- **DefaultShell**

Specifies the default shell that Privileged Access Manager assigns to a new UNIX user if no value is entered. If specified, the value for this token overrides the value in the client `lang.ini` file.

**Default:** `/bin/sh` (or `/sbin/sh` on HP-UX)

- **Dictionary**

Defines the full pathname of the file containing the words that *cannot* be used as passwords.

#### NOTE

To use this file, you must set the dictionary format password rule (`use_dbdict`) to *file* and set `UseDict` setting to `yes`. If the dictionary format is set to *db*, passwords that cannot be used are taken from the Privileged Access Manager database and this setting is ignored. This value is the default on UNIX.

#### WARNING

This token is obsolete. Use `dictionary` in the database instead.

**Default:** `/usr/dict/words`

- **GeneratePasswd**

Specifies whether `sepass` generates a new password by itself.

Valid values are `yes` and `no`.

**Default:** `no` (the user is asked to enter a new password.)

- **HomeDirUpd**

Specifies whether Privileged Access Manager updates the group ownership of the home directory of the user when the primary group of the user changes.

Valid values are **yes** and **no**

**Default:** `yes`

- **nis\_env**

Specifies whether the local host is an NIS or NIS+ client.

Valid values are no, nis, or nisplus.

**Default:** no

- **NisPlus\_server**

Specifies whether this station is an NIS+ server.

Valid values are yes and no.

If token value is yes, Privileged Access Manager treats password replacements as NIS+ password replacements.

**Default:** no

- **only\_local**

Determines whether the default setting for sepass includes the -l flag.

Valid values are yes and no.

If this token is set to yes, sepass replaces the password only in the local files. Example: the local password file (usually /etc/passwd), security files, and the local database

**Default:** no

- **only\_pmdb**

Specifies whether the default setting for sepass includes the -p flag. If token value is yes, it instructs sepass to change the password only on the PMDB at the host specified.

If no such database is defined, sepass does nothing.

**Default:** no

- **passwd\_distribution\_encryption\_mode**

Specifies which method is used to encrypt user passwords when passwords are distributed as part of the Policy Model service.

Valid values are:

**1** - Compatibility mode, to distribute passwords between Privileged Access Manager systems that do not use long passwords (This includes all machines running pre-r12.0 versions of Privileged Access Manager.)

**2** - MD5 mode, to distribute passwords between Privileged Access Manager systems that use long passwords and are also running Linux.

**3** - Bidirectional mode, to distribute passwords securely, as clear text within encrypted messages, between any Privileged Access Manager systems that use long passwords.

**Default:** 1

- **passwd\_format**

Indicates whether the password changes are propagated to an NT host.

Setting this token to **NT** means that one of the hosts you are administering is an NT host.

**Default:** none

- **passwd\_local\_encryption\_method**

Specifies which method is used to encrypt user passwords when storing these passwords locally.

Valid values are:

**crypt** - The standard one-way UNIX encryption that uses only the first eight characters of the password (as a DES key). Specifying crypt disables the use of long passwords.

**md5** - MD5 hash function that can encrypt passwords of indefinite length. Specifying md5 enables the use of long passwords.

**Default:** crypt

- **PromptOldPassword**

Specifies whether to prompt local users for their old password when sepass is invoked through /opt/CA/PAMSC/bin/segrace. (You must use the full path).

**Default:** yes (indicates that the users are prompted for their old passwords)

- **quiet\_mode**

Specifies whether sepass displays a copyright notice and a message about propagating passwords to Policy Models.

**Default:** no

- **RootPwAsOwn**

Specifies whether sepass lets a privileged user change the root password as if changed by root (using the -x option).

Valid Values are:

**yes**-Privileged users can use `sepass` to change the root password as if changed by root. They cannot change the root password as themselves (administrative change).

**no**-Privileged users can use `sepass` to change the root password only as themselves (administrative change).

For example, a privileged user can use the following command to change the root password if this token is set to **yes**:

```
sepass -x root
```

The same user cannot use the following command to change the root password:

```
sepass root
```

If this token is set to *no*, the opposite is true.

**Default:** no

- **SaveGroupAttrs**

Specifies whether the previous group file owner, group, and mode are preserved after an update of a group in the UNIX environment.

Valid values are yes and no.

**Default:** no (new values are set to 0, 0, 644 respectively)

- **SavePasswdAttrs**

Specifies whether the previous password file owner, group, and mode are preserved after an update of a user in the UNIX environment.

Valid values are yes and no.

**Default:** no (new values are set to 0, 0, 644 respectively)

- **Shadow\_Admin\_Change**

(AIX platforms only). Specifies whether the ADMCHG flag gets added to the user entry in the `/etc/security/passwd` file when an administrator changes the password from `selang` or using `sepass`.

**Default:** no

- **UIDAlgorithm**

Specifies which free UID algorithm to employ when adding new users. Setting it to any other value would select the older process. The *new* algorithm provides for UID numbers over 4 KB and is faster.

**Default:** new

- **UseDict**

Specifies whether to use the dictionary file (set with the Dictionary setting) when verifying a password.

**NOTE**

To use the dictionary file, you must also set the dictionary format password rule (`use_dbdict`) to *file*. If the dictionary format is set to *db*, passwords that cannot be used are taken from the Privileged Access Manager database and this setting is ignored.

**Default:** no

- **YpGrpCmd**

Specifies the command to use for generating the NIS group map.

**Default:** make group

- **YpMakeDir**

Specifies the name of the makefile directory to use when creating NIS maps.

**Default:** /var/yp

- **YpPassCmd**

Specifies the command to use for generating the NIS password map.

**Default:** make passwd

- **YpServerGroup**

Specifies the group file from which the NIS group map is made.

**Default:** /etc/group

- **YpServerPasswd**

Specifies the password file from which the NIS password map is made.

**Default:** /etc/passwd

- **YpServerSecure**

Specifies the name of the security file containing passwords that is used for building the NIS password map.

**Default:** Varies by platform:

- IBM AIX: /etc/security/passwd
  - HP-UX: /.secure/etc/passwd
  - Sun Solaris: /etc/shadow

- **YpTimeOut**

Specifies the time, in seconds, that a new client (selang, Security Administrator, and so forth) can run the ypbind test. The ypbind test determines whether the local host is connected to a NIS server. At expiration, the client exits and an error message appears.

The default value of zero (0) means that no ypbind test is conducted.

**Default:** 0

## pmd1

In the [pmd] section, the tokens are used to configure the generic Policy Model settings.

- **ClientOperationTimeout**

Defines the number of seconds a Policy Model client waits for a response from the Policy Model. If the Policy Model does not respond within this time frame, the client assumes that the Policy Model is non-responsive.

**Default:** 60 seconds

- **is\_maker\_checker**

Specifies whether to use Dual Control. If yes is selected, then the database cannot be updated directly, but only through a policy model database by a pair of administrators - a Maker and a Checker, who must collaborate on the update.

**Values:** yes, no

**Default:** no

- **min\_retries**

Specifies the minimum number of attempts that are made by sepmd to access an unavailable subscriber before giving up and temporarily shutting itself down.

**Default:** 4

- **pass\_auth**

Specifies whether sepass verifies the invoker password during a remote password change. The sepass utility compares the old password that the user enters with the password stored in the local database. If this token is set to yes, then sepass also compares the old password that the user running sepass enters with their own password as it is stored in the remote database (pmdb). This means that the sepass user must enter their own password even when changing the password for another user.

**Values:** yes, no

**Default:** yes

- **pmd\_backup\_directory**

Specifies the directory to store Policy Model backups. Each Policy Model backup is stored in a subdirectory named <pmd\_name>.

**Default:** /opt/CA/PAMSC/data/policies\_backup

- **pmd\_directory**

Specifies the directory in which the policy model database resides. Each policy model database resides in the <pmd\_directory>/<pmd\_name> subdirectory where <pmd\_name> is the policy model name.

**Default:** /opt/CA/PAMSC/policies

- **pull\_option**  
Specifies that the local host, and any policy model on this station, have a parent policy model to which they subscribe. When this station becomes temporarily unavailable to send updates, the pull\_option token enables Privileged Access Manager agent to send a message to these parent policy models when this station becomes available again. Then the parents start sending updates immediately, instead of waiting for the next retry.  
**Values:** yes, no  
**Default:** yes
- **QD\_timeout**  
Specifies the maximum time (seconds) that the daemon sepmd waits to update a subscriber database during the first scan of the subscribers. If the maximum time elapses and the daemon fails in updating a subscriber, then it skips to the remaining subscribers.  
**Default:** 3
- **retry\_timeout**  
Specifies the time (minutes) between consecutive attempts to access an unavailable subscriber.  
**Default:** 30 minutes
- **send\_unix\_env**  
Specifies the token when set to yes, the *sepmd -n* option sends the content of the policy model password files and group files.  
**Values:** yes, no  
**Default:** yes
- **ShutdownWaitingTimeout**  
Defines the number of milliseconds a Policy Model waits for its components to shut down gracefully. If Policy Model components do not shut down gracefully within this time frame, the Policy Model forces them to shut down.  
**Default:** 60 milliseconds
- **shutoff\_time**  
The time (in minutes) sepmd waits before shutting itself off. If this token is set to zero, sepmd never shuts itself off.  
**Default:** 0
- **updates\_in\_chunk**  
Specifies the maximum number of commands that the Policy Model sends to each subscriber every cycle. The Policy Model sends commands to its subscribers one by one in a loop.  
**Default:** 10

## policyfetcher

In the [policyfetcher] section, the tokens control the behavior of the policy fetcher daemon (policyfetcher).

- **check\_deployment\_tasks**  
Defines how often, in seconds, policyfetcher checks for new deployment tasks (DEPLOYMENT resources) on the Distribution Host.  
**Default:** 600 (every 10 minutes)  
**Limits:** A minimum value of 60
- **deploy\_timeout**  
Defines the number of seconds policyfetcher waits for a deployment or undeployment task to complete on the endpoint.  
**Default:** 900
- **devcalc\_command**  
Defines the selang command that policyfetcher uses to run the deviation calculation.  
**Default:** start DEVCALC params(-nonotify)

**Example:** start DEVCALC params(-nonotify -precise)

- **dh\_command\_retry\_interval**  
Defines the number of seconds between each DH notification command retry.  
**Default:** 60
- **endpoint\_heartbeat**  
Defines the frequency at which policyfetcher sends a heartbeat to the Distribution Host (DH). The frequency is a factor of the check\_deployment\_task setting, and determines how many times policyfetcher checks deployment tasks before it sends a heartbeat. For example, if check\_deployment\_task is set to the default 600 seconds (10 minutes) and you set this to 6, policyfetcher sends a heartbeat every 3600 seconds (1 hour).  
The policyfetcher runs the deviation calculator (start devcalc command) after sending the heartbeat, and then waits 60 seconds for the deviation calculation to complete. After 60 seconds, policyfetcher continues to check that local endpoint information is identical to DH information.  
**Default:** 6
- **max\_deployment\_errors**  
Defines the maximum number of deployment errors that the endpoint sends to the DMS.  
**Default:** 10
- **max\_dh\_command\_retry**  
Defines the maximum number of times policyfetcher retries to get update notifications from DH before giving up.  
**Default:** 10
- **max\_dh\_retry\_cycles**  
Defines the maximum number of cycles policyfetcher retries to get update notifications from production DHs before moving to disaster recovery DHs.  
**Default:** 5
- **policy\_verification**  
Specifies whether the policyfetcher daemon verifies new deployment tasks on a backup Privileged Access Manager database before executing the tasks.  
Valid values:  
1 - Run policy verification  
0 - Disable policy verification  
**Default:** 0
- **policyfetcher\_enabled**  
Specifies whether to run the policyfetcher daemon.  
Valid values:  
1 - Run policyfetcher  
0 - Disable policyfetcher  
**Default:** 0

#### NOTE

To run policyfetcher on UNIX, specify value 1 for policyfetcher\_enabled token. To run policyfetcher on Windows, specify value 1 for policyfetcher\_enabled token and enable the registry value at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications\Policyfetcher
```

## PUPMAgent

In the [PUPMAgent] section, the tokens determine the functionality of the Privileged User Password Management Agent.

- **EnableLogonIntegration**  
Specifies that terminal integration is enabled.  
**Limits:** 0, terminal integration is disabled; 1, terminal integration is enabled.  
**Default:** 1
- **Endpointname**



Specifies the name of an endpoint on the local server used for the PUPM login integration.

**Default:** <Short local host name>

**IMPORTANT**

If the specified Endpointname value is greater than 15 characters, login integration fails.

- **InterfaceName**

Defines the communication interface name. This name is the UNIX socket name with which the SAM Agent handles requests. The socket file is located in the /opt/CA/PAMSC/data/PUPMAgent directory.

**Default:** PUPMAgentInterface

- **OperationMode**

Specifies the SAM Agent work mode.

**Limits:** 0, the SAM Agent is disabled and not running. 1, the SAM Agent is enabled, running but not logging data to trace files. 2, the SAM Agent is enabled, running, and logging data to trace files.

**Default:** 0

## seagent

In the [seagent] section, the tokens control the behavior of the seagent daemon.

- **debug\_backup\_dir** Specifies the backup debug files location.

**Default:** Privileged Access Manager product log directory

- **debug\_backup\_num**

Defines the number of backup debug files to save.

**Value:** A positive number

**Default:** 2

- **debug\_file**

Defines the name of the file to which Privileged Access Manager writes seagent debug messages.

**Default:** *ACInstallDir/log/seagent\_debug*

- **debug\_level**

Specifies the minimal level of debug messages that Privileged Access Manager writes to the debug file.

**Limits:**

- disabledno messages are written to the debug file
- criticalCRITICAL messages are written to the debug file
- very\_highCRITICAL and VERY\_HIGH messages are written to the debug file
- highCRITICAL, VERY\_HIGH, and HIGH messages are written to the debug file
- normalCRITICAL, VERY\_HIGH, HIGH, and NORMAL messages are written to the debug file
- lowCRITICAL, VERY\_HIGH, HIGH, NORMAL, and LOW messages are written to the debug file

**Default:** critical

- **watchdog\_check\_interval**

Defines the time interval, in seconds, at which seagent checks that seoswd exists.

**Note:** This token applies only if there is a high volume of incoming connections to seagent. If seagent is idle, it checks that seoswd exists every 3 seconds and this token is ignored.

**Default:** 30

## segrace

In the [segrace] section, the tokens determine the attributes of the segrace utility.

- **sepass\_command**

Specifies the location of the Privileged Access Manager password replacement command that is executed when a user has no remaining grace logins.

**Default:** *ACInstallDir/bin/sepass*

## seini

In the [seini] section, the tokens determine the attributes of the seini intelligent search feature.

- **get\_error\_warning**  
Specifies whether the error and warning messages for the intelligent search feature display.  
**Default:** yes
- **perform\_action**  
Specifies whether seini performs its operations on the token or section found by the intelligent search feature.  
Valid values are yes and no.  
If this token is set to **yes**, the section and token, found by the additional intelligent search, are used for the requested seini operation.  
**Default:** no
- **use\_intelligent\_search**  
Specifies whether to perform an intelligent search when you invoke the seini utility.  
**Default:** no

## selock

In the [selock] section, the tokens control the behavior of the selock utility.

- **unlocking\_user**  
Specifies the name of a user, other than the owner, who can unlock a locked screen.  
**Default:** root

## selogrd

In the [selogrd] section, the tokens control the behavior of the log routing daemons selogrd and selogrcd.

- **Caudit\_size**  
Specifies the maximum size, in KB, of the audit collection file, before selogrcd creates a backup file and opens a new file.  
The minimum value is 50 KB.  
**Default:** 1024
- **CBackUp\_Date**  
Sets the criterion by which selogrcd performs the backup.  
Valid values include: none, yes, daily, weekly, and monthly.  
If you specify **yes**, Privileged Access Manager performs backups according to the size limit token Caudit\_size and timestamps the file.  
If you specify **none**, Privileged Access Manager performs the backup according to the Caudit\_size token but it does not timestamp the file.  
If you specify **daily**, **weekly**, or **monthly**, selogrcd adds a timestamp when it first creates the file. When the current date passes the timestamp, Privileged Access Manager automatically creates a backup file and timestamps it. However, if the size of the file exceeds the value of the Caudit\_size token first, Privileged Access Manager creates a backup file without issuing a timestamp.  
**Default:** NONE
- **ChangeLogFactor**  
Specifies the factor applied to the value in the token *Interval* before testing whether the log file was changed to a backup file. For example, if the *Interval* token is set to 5 and the *ChangeLogFactor* token is set to 5 (the default), Privileged Access Manager waits 25 seconds before checking whether the log file was changed to a backup file.

**Default:** 5

- **CipherName**

Specifies the name of the file that contains the encryption functions used by selogrd if the UseEncryption token is set to eTrust.

This file must be placed in the *ACInstallDir/lib/* directory.

The CipherName is a symbolic link to a shared object file.

**Default:** adcipher

- **CollectFile**

Specifies the name of the file in which the audit collector daemon selogrcd stores the collected audit records.

**Default:** *ACInstallDir/log/seos.collect.audit*

- **CollectFileBackup**

Specifies the name that selogrcd uses when backing up and renaming the file of collected audit records when it receives the USR1 signal.

**Default:** *ACInstallDir/log/seos.collect.bak*

- **ConsolePort**

Specifies the name or port number for selogrd - secmon communication. This token is necessary only if you plan to run both selogrcd and secmon on the same host.

If specified, selogrd - secmon communication is done using the specified port. Otherwise, they use the port that is specified in the *ServicePort* token, or they use RPC portmapper to allocate a port dynamically if that token is also empty. The service name must be a UDP port because the log routing daemon uses UDP for communication.

If the token value is a number, daemons bind to the specified port number.

If the token value is a service name (string), /etc/services or NIS services maps are used to resolve the port number.

**Default:** Token not set (value taken from *ServicePort* token)

- **DataFile**

Specifies the name of the file to which the target routing information is written before being delivered to the specified targets.

**Default:** *ACInstallDir/log/logroute.dat*

- **Interval**

Specifies the time interval, in seconds, between each poll of the log file by the selogrd daemon.

**Default:** 5

- **KeyFile**

Specifies the name of the file that holds the audit encryption key.

This key is used when selogrd performs Privileged Access Manager audit encryption. The location of the key file is the *ACInstallDir/lib* directory.

The key can be changed by sechkey utility.

**Default:** adcipher.bin

- **Mailer**

Specifies the name of the program that selogrd uses to send email.

**NOTE**

This option is relevant only if you set the UseSmtplib token to yes.

**Default:** /bin/mail

- **MaxErrorSending**

Specifies whether selogrd sends error messages to syslog regarding difficulties sending audit records to selogrcd, only after the number of difficulties surpasses this token value.

The default value is 1: every time selogrd has difficulties sending to selogrcd, it sends a message to syslog.

**Default:** 1

- **MaxSeqNoSleep**

Specifies the maximum number of log records scanned by selogrd without sleeping.

**Default:** 50

- **RefuseUnencrypted**

Specifies whether selogrcd accepts unencrypted audit. It is used with the UseEncryption token and is redundant if UseEncryption is set to **no**. It is therefore applicable only if selogrcd uses encryption.

Valid values are:

**yes**- refuse unencrypted audit

**no**- accept both encrypted and unencrypted audit

**Default:** no

- **ReopenInterval**

Specifies the time (seconds) that selogrd waits to reopen the audit file.

**Default:** 20

- **RouteFile**

Specifies the name of the log routing configuration file. The file is used unless overridden by the -config option of the selogrd utility.

**Default:** *ACInstallDir/log/selogrd.cfg*

- **SavePeriod**

Specifies the time interval, in minutes, between saving information about the number of records sent.

**Default:** 2

- **sendmail\_header\_format**

Determines the user name format in the header of mail that selogrd sends.

**Note:** Change this token value only if selogrd cannot send mail. (That is, if you see an error 4634 from selogrd in your syslog.)

Valid values include the following:

**1**-The user name format is *SmtplibMailFrom*

For example: eTrust\_Admin

**2**-The user name format is *SmtplibMailFrom@hostname* (where *hostname* is the host which selogrd runs on).

For example: eTrust\_Admin@machine

**Default:** 1

- **ServicePort**

Specifies the name or port number that the log routing facility must use.

If specified, selogrd and selogrcd use the specified port. Otherwise selogrd and selogrcd use the RPC portmapper to allocate a port dynamically.

If the token has a value, selogrd and selogrcd use the specified port. Otherwise, selogrd and selogrcd dynamically allocate a UDP port using the RPC portmapper. The service name must be a UDP port because the log routing daemon uses UDP for communication.

If the token value is a number, daemons bind to the specified port number.

If the token value is a service name (string), /etc/services or NIS services maps are used to resolve the port number.

Only a UDP port/service can be specified.

**Default:** Token not set (selogrd and selogrcd use RPC portmapper to allocate a port dynamically).

- **SmtplibMailFrom**

Specifies the identity of the sender for UseSmtplibMail.

**Default:** AccessControl\_Admin

- **SmtplibMailServer**

Specifies the address of the remote mail server host. Use this token if UseSmtplibMail is set to yes. If you do not specify this token, the local computer is assumed to be the mail server.

**Default:** (blank - local server)

- **SmtplibTimeLimit**

Specifies the time limit, in seconds, that selogrd waits for the mail server to answer before timing out.

**Default:** 100

- **tec\_conf\_file**

Specifies the name of the configuration file that is used for the TEC event creation by the selogrd daemon.

**Default:** /etc/tecad\_seos.conf

- **UseEncryption**

Determines the type of encryption.

Valid values include the following:

**native**-selogrd uses Privileged Access Manager standard encryption.

**eTrust**-selogrd uses audit log encryption through adcipher.

**no**-selogrd does not use encryption.

**Default:** no

- **UseSmtplib**

Determines whether to use the direct mail feature or the previous Mailer.

**Default:** yes

## seos

In the [seos] section, the tokens determine the global settings that are used by Privileged Access Manager.

- **admin\_data**

Specifies the directory where the Privileged Access Manager Security Administrator rulers and other configuration files are stored.

**Default:** *ACInstallDir/data*

- **auth\_login**

Determines the login authority method. Valid values are:

**native** - login checks the user password against the UNIX passwd or shadow file.

**eTrust** - when the user does not exist in the Native environment, checks the user password against the Privileged Access Manager database.

**PAM** - when the user does not exist in the Native environment, checks the login through the PAM module. This is only supported on machines where PAM is supported. PAM is used to validate the user for users such as LDAP-defined users.

**Default:** native

- **auth\_module\_names**

Defines the language client module that is allowed to authenticate outside of native authentication. The client inside the lca API calls set this token before the authentication. Changing this token can affect other clients authenticating in non-native mode.

No default.

- **fast\_create\_db**

Specifies whether the PMDB uses the fast database copy device.

Valid values are:

**no** - Use the old device.

**yes** - Use the fast database copy device.

**Default:** yes

- **full\_year**

Specifies the format for displaying the year using four digits or last two digits.

For example, setting the token to yes displays 2000 instead of 00.

The following values are valid:

**yes**-four digits

**no**-two digits

This token influences the output that is produced by secons -tv, dbmgr -d, and the seaudit utility.

**Default:** yes (four-digit)

- **ldap\_base**

Defines the distinguished name of the search base for user data queries in the LDAP Directory Information Tree (DIT) by Privileged Access Manager LDAP-enabled utilities (such as sebuildla).

For example, use the following format, replacing inputs with your own:

```
o=organization_name,c=country_name
```

**Default:** Token not set

**WARNING**

To set up `sebuildla` and the required LDAP configuration settings, be familiar with LDAP and be able to execute the `ldapsearch` command. We recommend that you read the man pages for `ldap(1)`, `ldapsearch(1)`, and the information about setting up in the documentation for your LDAP client.

- **ldap\_hostname**

Defines a space-separated list of the host names where the LDAP servers are running for Privileged Access Manager LDAP-enabled utilities.

**Default:** Token not set (localhost).

- **ldap\_certdb\_path**

Defines the directory where the Netscape-style certificate database is located.

This token is required for `sebuildla` on platforms that use the Netscape LDAP SDK API for LDAP over SSL (Solaris).

For `sebuildla` to work, a certificate database must contain a valid certificate for the LDAP server.

**NOTE**

`sebuildla` uses LDAP over SSL with server authentication (that is, no client authentication). Consult your PKI toolkit documentation for details on setting up secure services.

**Default:** `/.netscape`

- **ldap\_keydb**

Defines the name of the key database file.

**NOTE**

This setting is for AIX only as an AIX key database can have an arbitrary name. In contrast, Netscape security databases have names like `certX.db` and `keyY.db` depending on the implementation version, and so only the `ldap_certdb_path` is required for finding them.

**Default:** Token not set

- **ldap\_method**

Specifies the bind method that Privileged Access Manager uses for LDAP-enabled utilities to access the LDAP service. By default, `sebuildla` uses *simple* authentication with all security mechanisms. In simple authentication, `ldap_userdn` and the corresponding credential are passed to the LDAP server. `sebuildla` stores user credentials in encrypted form in `ldapcred.dat` at `ACInstallDir/etc`. These two parameters approximate the account and password combination that the LDAP server requires.

**NOTE**

For SASL or TLSv.1/SSL, consult your LDAP server documentation. For a particular `ldap_method` setting to take effect, the corresponding mechanism must be supported and configured in the native LDAP client that is deployed on the computer where `sebuildla` is executed. That is, with TLS/SSL operations, valid certificates should be installed on the server and client side.

Valid values are:

**0-** Standard LDAP

**1-**SASL (RFC 2222)

**2-**LDAPS (LDAP over SSL - server authentication only.)

**NOTE**

The method that you use determines how you set up the `ldap_userdn` token and its corresponding credential (through `seldapcred` utility).

**Default:** 0

- **ldap\_port**

Defines the LDAP server port for Privileged Access Manager LDAP-enabled utilities. Change this token if your LDAP server is not using the standard LDAP port (389).

**Default:** Token not set (389).

- **ldap\_query\_size**

Defines the maximum number of LDAP entries sebuildla retrieves in each batch query.

Use this token when you do not want to change the LDAP server-side size limit parameter. Typically, sebuildla attempts to retrieve all data in one instance. If there are numerous user entries, the amount of data might exceed the size limit of the server and might cause the LDAP operation to fail. If you set `ldap_query_size`, sebuildla need not retrieve all entries for the operation to succeed. If the total number of user entries is greater than either the `ldap_query_size` or the server-side size limit, the number of entries that are retrieved corresponds with the lower number of these two settings.

**WARNING**

Enabling batch queries can affect sebuildla performance. Consider using this setting only where the LDAP environment has numerous user data (thousands of entries) in the DIT (Directory Information Tree).

**NOTE**

For information about server-side LDAP controls, for example, the OpenLDAP server (slapd) `sizelimit` parameter, consult your LDAP server documentation. **Default:** Token not set (empty)

- **ldap\_timeout**

Defines the maximum amount of time (in seconds) that Privileged Access Manager LDAP-enabled utilities wait when binding to the LDAP service and obtaining LDAP search results, before terminating the connection. The time that it takes to retrieve information from the LDAP service depends on how fast the LDAP service is, and how much user data is stored in the DIT. Use this token to account for these aspects.

**NOTE**

You might also need to adjust server-side LDAP controls to avoid truncated search results. For example, for the OpenLDAP server (slapd) adjust the `sizelimit` parameter. Consult your LDAP server documentation for more information.

**Default:** Token not set (15 seconds)

- **ldap\_uid\_attr**

Defines the name of the attribute that contains the user name in the LDAP DIT. RFC 2307 (An Approach for Using LDAP as a Network Information Service) prescribes *uid* as this attribute, which is the default value for this token. Change this token to let Privileged Access Manager LDAP-enabled utilities operate against LDAP DITs with nonstandard schemas.

**Default:** Token not set (uid).

- **ldap\_uidNumber\_attr**

Defines the name of the attribute that contains the UID number in the LDAP DIT. RFC 2307 prescribes *uidNumber* as this attribute, which is the default value for this token. Change this token to let Privileged Access Manager LDAP-enabled utilities operate against LDAP DITs with nonstandard schemas.

**Default:** Token not set (uidNumber).

- **ldap\_user\_class**

Defines the name of the object class that contains the user data in the LDAP DIT. RFC 2307 prescribes *posixAccount* as this object class, which is the default value for this token. Change this token to let Privileged Access Manager LDAP-enabled utilities operate against LDAP DITs with nonstandard schemas.

**Default:** Token not set (posixAccount).

- **ldap\_userdn**

Defines the distinguished name (DN) of the LDAP user that Privileged Access Manager LDAP-enabled utilities use for retrieving user data from the LDAP DIT. Based on RFC 2307, Privileged Access Manager expects to find the user data in the *uid* and *uidNumber* attributes of the *ou=People* level in the DIT. For security reasons, we recommend that this user (`ldap_userdn`) is given access to this data only.

If anonymous access to the DIT is permitted, you can keep this token empty. Otherwise, you set this token and run the `seldapcred` utility for Privileged Access Manager LDAP-enabled utilities to authenticate to the LDAP service. Only do this once, as `seldapcred` stores your encrypted credential in a file for reuse.

For example, set this token as follows:

```
ldap_userdn = uid=user1,ou=People,dc=myCompany,dc=com
```

**Default:** Token not set

- **ldap\_userinfo\_ladb**

Specifies whether to retrieve user information from the LDAP Directory Information Tree (DIT).

**Limits:** yes, no

**Default:** no

- **ldap\_verbose**

Specifies whether to enable detailed account of LDAP operations that are involved in sebuildla getting user data.

Use this setting when you set up LDAP data retrieval in sebuildla or when troubleshooting.

Valid values are **0**-disabled; a non-zero integer-enabled.

**Default:** 0

- **locale**

Determines the language for the Privileged Access Manager daemons and utilities. Privileged Access Manager can function in several languages.

Supported languages include: C, Japanese, Chinese-s, Chinese-t

For the complete list of languages, see `/etc/ca/localeX/calocmap.txt`; on Linux, see `/opt/CA/SharedComponents/cawin/locale/`.

**Default:** C

- **pam\_enabled**

Valid on SOLARIS, HP-UX, and LINUX only.

Specifies whether the local host enables use of PAM for authentication and password changes in the LDAP database.

To do that, it checks whether the PAM library can be dynamically loaded (the library must exist on your system).

Valid values are: 'no', 'yes'.

**Default:** yes

- **parent\_pmd**

Defines a comma-separated list of policy model databases (PMDBs) from which this computer accepts updates. The local Privileged Access Manager database rejects updates from any PMDB that is not specified in this list.

You can also specify a file path that contains a line-separated list of PMDBs.

Set this token to `"_NO_MASTER_"` for the local Privileged Access Manager database to accept updates from any PMDB.

If you do not set this token, the local Privileged Access Manager database does not accept updates from any PMDB.

Each PMDB is specified in the following format: `pmd_name@hostname`

For example:

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
```

```
parent_pmd = /opt/CA/PAMSC/parent_pmdbs_file
```

**Default:** Token is not set (database does not accept updates from any PMDB).

**Note:** sepass does not support multiple destinations on the parent\_pmd token.

- **passwd\_pmd**

Specifies the PMDB to which sepass sends password updates.

If you do not set this token, it inherits the value of the parent\_pmd token.

The format is `pmd_name@hostname`.

The parent\_pmd and passwd\_pmd tokens can have the same value. If the values in the parent\_pmd and passwd\_pmd tokens are not the same, the passwd\_pmd database sends its updates to the parent\_pmd database for distribution.

Therefore, the parent\_pmd database must be a child (subscriber) of the passwd\_pmd database.

No default.



**Note:** sepass does not support multiple destinations on the passwd\_pmd token.

- **ReverseIpLookup**

Controls the way seagent identifies the connecting client.

The following values are valid:

**yes**-seagent looks up the IP address of the socket of the open client.

**no**-seagent uses the host name as received from the client; seagent does not resolve any host names. (The same effect can be achieved by disabling class `TERMINAL`.)

**Default:** yes

- **secondary\_pmd**

Specifies the PMDB used as the secondary target for password replacement for users who are not defined in the primary target (passwd\_pmd).

The format is *pmd\_name@hostname*.

No default.

- **SEOSPATH**

Specifies the directory in which Privileged Access Manager is installed.

You can install Privileged Access Manager in any directory, *if* it is not *on* an NFS-mounted file system.

**Default:** *ACInstallDir*

- **SyncUnixFilePerms**

Specifies whether Privileged Access Manager synchronizes its ACL permissions with the ACL and other permissions of the native UNIX system, if they exist.

The following values are valid:

**no**-Do not synchronize the UNIX file permissions with Privileged Access Manager ACLs.

**warn**-Do not synchronize ACL permissions, but issue a warning if the permissions in Privileged Access Manager and UNIX conflict.

**traditional**-Change rwx permissions for the group and the owner according to Privileged Access Manager ACLs, issue a warning in all other cases.

**acl**-Change native file-system ACLs according to Privileged Access Manager ACLs (on platforms that support ACLs).

**force**-Functions the same as traditional or acl (on platforms that support ACLs), but also forces mapping defaccess to "other" permissions.

**Note:** On HP-UX and Sun Solaris 2.5 (and above), support is provided for the file system ACLs. On other platforms and operating system versions, only traditional permissions mode of a file are supported.

**Default:** no

- **TRUEPATH**

Specifies the directory where Privileged Access Manager is physically located. The Privileged Access Manager directory may be a symbolic link to another physical location. This token points to the actual physical location where Privileged Access Manager is installed.

**Default:** *ACInstallDir*

- **use\_rpc\_protocol**

Determines whether the RPC portmapper is required. The presence of the RPC portmapper is required if you want to use the old (1.43) Privileged Access Manager protocol. The old protocol is required to support NIS+ password changes.

This token replaces the old\_protocol token.

The following values are valid:

**yes**-Use the RPC portmapper to assign the port.

**no**-Use the port that is specified by the ServicePort token.

**Default:** no

## SEOS\_syscall

In the [SEOS\_syscall] section, SEOS\_syscall kernel module uses the following tokens.

- **bypass\_NFS**

Determines whether to bypass NFS files from SEOS events.

Valid values:

**0**-Do not by pass NFS files

**1**-Bypass NFS files

**Default:** 0

- **bypass\_realpath**

Specifies whether to bypass the real file paths resolution for authorization.

If you enable this setting (1), Privileged Access Manager does not resolve file paths for authorization. This accelerates file events handling. However, generic rules are not enforced for file accesses that are made using links.

**Example:** A deny access rule for /realpath/files/\* is not considered if this setting is enabled and a user accesses a file in this directory from a link. Create a generic rule for the link too (/alternatepath/\*).

**Default:** 0 (disabled)

- **cache\_enabled**

Determines whether to use caching for full path resolution to determine access permissions for files.

Valid values:

**0**-No caching

**1**-Use caching

**Default:** 0

- **cache\_rate**

Determines the cache rate that used when the cache is enabled for full path resolution.

Bigger values mean better caching.

**Default:** 10000

- **cache\_realpath**

Specifies whether to cache the resolved full path.

**Values:** 0 (no caching), 1 (use caching)

**Default:** 0

- **call\_tripAccept\_from\_seload**

Determines whether to call tripAccept from the seload command after Privileged Access Manager starts. If tripAccept is called, defines a list of comma-separated TCP/IP ports that tripAccept should connect to, and wake up the listeners of the ports.

Valid values:

**1 to 64000** - Any TCP/IP port number

**0**-Do not call tripAccept from seload.

**Limits:** 0-64000

**Default:** 0

- **cdserver\_conn\_res**

Determines whether to treat T\_CONN\_RES streams messages as high priority messages in the fiwput routine on UnixWare.

Valid values:

**1**-handle T\_CONN\_RES streams messages as high priority messages in the fiwput routine.

**0**-handle T\_CONN\_RES streams messages as low priority messages in the fiwput routine.

**Default:** 0 (1 on UnixWare)

- **debug\_protect**

Determines whether to allow debugging of any program while Privileged Access Manager is running.

Valid values:

**0**-Debugging allowed

**1**-Debugging not allowed

**Default:** 1

- **DESCENDENT\_dependent**

Determines whether a descendent of a SEOS daemon can register a SEOS service.

Valid values:

**0**-Anyone can register a SEOS service

**1**-Only a descendant can register a SEOS service

**Default:** 0

- **dtrace\_coexistence**

Defines how Privileged Access Manager co-exists with dtrace. If dtrace is installed and set to monitor syscalls, it loads the systrace kernel module. This module interacts with Privileged Access Manager with undefined results and can cause system panic or syscall interception problems.

**Default:** 0 (dtrace is prevented from loading)

Valid values:

**0**-Privileged Access Manager prevents dtrace from loading the systrace kernel module.

**1**-Dtrace loads the Systrace kernel module. In this case you must ensure that your system loads the modules and Privileged Access Manager in the following order:

1. a. Load and start Privileged Access Manager (seload)
- b. Load systrace (modprobe systrace)
- c. dtrace system calls
- d. Unload systrace (rmmod systrace)
- e. Stop Privileged Access Manager (secons -sk)
- f. Unload Privileged Access Manager (SEOS\_load -u)

**WARNING**

Loading systrace and Privileged Access Manager in a different order can result in system panic or syscall interception problems.

- **exec\_read\_enabled**

Specifies whether the Privileged Access Manager kernel identifies script execution.

Valid values:

**0**-Privileged Access Manager kernel does not identify script execution.

**1**-Privileged Access Manager kernel identifies script execution.

**Default:** 0

- **file\_bypass**

Indicates whether Privileged Access Manager checks file access for files that are not defined in the database. By default Privileged Access Manager does not check files that are not defined in the database.

Valid values:

**-1**-Do not check all files

**0**-Check all files

**Default:** -1

- **file\_rdevice\_max**

Defines the maximum number of devices in the device protection table.

**Default:** 0-Privileged Access Manager does not protect system devices.

**Note:** We recommend that you specify a minimum of 20 system devices.

- **GAC\_root** Determines whether to use GAC caching for files when the user is root. By default GAC is not used when the user is root.

Valid values:

**0**-No caching for root user

**1**-Use caching for root

**Default:** 0

- **HPUX11\_SeOS\_Syscall\_number**

Determines the default syscall number to communicate with SEOS\_syscall on HP-UX.

Valid values include any unused syscall entry number in sysent.

**Default:** 254

- **kill\_signal\_mask**

Defines which signals to protect.

Valid values include a mask that ORs (includes) all the signals that we want SEOS events for.

**Default:** SIGKILL, SIGSTOP, or SIGTERM events

Actual value varies by platform:

- (HP-UX) 0x804100
- (Sun Solaris) 0x404100
- (IBM AIX and Digital DEC UNIX) 0x14100
- (Linux) 0x44100

- **LINUX\_SeOS\_Syscall\_number**

Determines the default syscall number to communicate with SEOS\_syscall on LINUX.

- **max\_generic\_file\_rules**

(Valid on AIX, HP, Linux, and Solaris only) Defines the maximum number of generic file rules allowed in the database.

**Note:** A large number may cause strange behaviors on different platforms. For assistance, contact CA Support at <http://ca.com/support>.

Valid values include any number greater than 511.

**Default:** 256

- **max\_regular\_file\_rules**

(Valid on AIX, HP, Linux, and Solaris only) Defines the maximum number of file rules allowed in the database.

**Note:** A large number may cause strange behaviors on different platforms. For assistance, contact CA Support at <http://ca.com/support>.

Valid values include any number greater than 4095.

**Default:** 4096

- **mount\_protect**

Determines whether to allow mount and unmount of directories used by Privileged Access Manager.

Valid values:

**0**-Allow mounting

**1**-Do not allow mounting

**Default:** 1

- **proc\_bypass**

Determines whether to check file access when a file belongs to a process file system (/proc).

Valid values:

**0**-Token is ignored

**1**-Bypass file access checks

**Default:** 1

- **SEOS\_network\_intercept\_type** (Valid on HP-UX 11.11, 11.23, 11.31, and Sun Solaris 8, 9, 10, 11)

Specifies the type of network interception to use.

**WARNING**

Configure SEOS\_use\_streams = yes. Do not modify the SEOS\_network\_intercept\_type token yourself. For assistance, contact Broadcom Support at <https://www.broadcom.com/support>.

Valid values:

**0**-TCP Hook

**1**-Streams

**2**-Network System Call

**Default:** 2

- **SEOS\_request\_timeout**  
Specifies the time to keep a request in the authorization queue.  
Valid values:  
**0** - Timeout is disabled  
**2 to 1000** - the timeout interval in seconds  
**Default:** 0  
**Note:** If the timeout is set to less than 2 seconds or more than 1000 seconds, Privileged Access Manager reverts to the default value (0). No timeout is applied.
- **SEOS\_streams\_attach**(Valid on HP-UX 11.11, 11.23, 11.31, and Sun Solaris 8, 9, 10, 11)  
Specifies whether Privileged Access Manager attaches the SEOS Streams to the open TCP streams during startup.If you change this setting, restart all daemons that already listen to the network for Privileged Access Manager to protect them.  
**Note:** To use SEOS\_streams\_attach, configure SEOS Streams as the network interception method.  
Valid values are yes and no.  
**Default:** yes
- **SEOS\_unload\_enabled**  
Determines whether the SEOS\_syscall kernel module can be unloaded.  
Valid values:  
**0**-Do not allow the unload  
**1**-Allow the unload  
**Default:** 1
- **SEOS\_use\_ioctl**  
Specifies the Privileged Access Manager kernel module communication method (ioctl or system call).You can use the ioctl communication method when all available system call numbers are in use by the operating system.  
  
**WARNING**  
Do not modify this token yourself. For assistance, contact Broadcom Support at <https://www.broadcom.com/support>.  
  
Valid Values:  
**0**-system call  
**1**-ioctl  
**Default:** 0
- **SEOS\_use\_streams**  
(Valid on HP-UX 11.11, 11.23, 11.31, and Sun Solaris 8, 9, 10, 11)  
Specifies whether to use streams subsystem for network interception.  
Valid values are yes and no.  
**Default:** no
- **silent\_admin**  
Defines the user IDs of the maintenance users. The activity of this user is permitted when security is down and silent\_deny is yes. To define the maintenance user, use the user numeric UNIX UID.  
**Default:** 0 (user ID of root)
- **silent\_deny**  
Determines whether to deny any event when security is down.  
Valid values:  
**yes**-Silent deny is enabled (maintenance mode)  
**no**-Silent deny is disabled  
**Default:** no
- **STAT\_intercept**  
Specifies whether to check file access when a STAT system call occurs.

Valid values:

**0**-Do not check file access

**1**-Check file access

If you specify 1 (check file access), Privileged Access Manager does not let users without read permissions perform operations that get information about a file. Such user attempts are recorded as "read" in the audit log. If you set this value to 0, any user without read access can get the file information.

**Default:** 0

- **STOP\_enabled**

Determines whether to use the STOP feature, which protects from stack overflow attacks.

Valid values:

**0**-Off

**1**-On

**Default:** 0

- **suid\_cache\_max**

Specifies the maximum number of entries in the setuid cache. The setuid cache is used for managing non-PAM ready login applications such as sftp.

**0**-The cache is disabled.

**Default:** 128

**Note:** Do not change this value unless directed by Broadcom staff. For assistance, contact Broadcom Support at <https://www.broadcom.com/support>.

- **synchronize\_fork**

Determines how fork synchronization is managed.

*Valid values on HP-UX platforms:*

**1**-Report forks from parent

**2**-Report forks from child

*Valid values on other platforms:*

**1**-Parent reports without synchronization

**2**-Parent reports with synchronization (not supported on Linux)

**Limits:** Any value lower than 1 is interpreted as 1. Any value greater than 1 is interpreted as 2.

**Default:** 1

**Note:** Do not modify this setting yourself because it may cause strange behaviors on different platforms. For assistance, contact Broadcom Support at <https://www.broadcom.com/support>.

- 

- **syscall\_monitor\_enabled**

Specifies whether Privileged Access Manager monitors processes that are executing Privileged Access Manager code. If you have this enabled (the default), you can use the secons -sc or secons -scl to view these processes.

Valid values:

**0**-inactive

**1**-active

**Default:** 1

- **threshold\_time**

Defines how long, in seconds, an intercepted system call can be blocked before it is considered risky. If a process is blocked for a period that is longer than this time, Privileged Access Manager reports that SEOS\_syscall module unload can fail.

**Note:** This value affects the unload readiness reports Privileged Access Manager provides. For more information, see the *Enterprise Administration Guide*.

**Default:** 60

- **trace\_enabled**

Determines whether to use the SEOS\_syscall circular trace buffer.

Valid values:

**0**-Do not use tracing

**1**-Use tracing

**Default:** 0

- **use\_tripAccept**

Determines whether to use the tripAccept utility when unloading SEOS\_syscall to wake up the blocked accept system calls. This avoids running SEOS\_syscall code after the module is unloaded.

Valid values are yes and no.

**Default:** yes

## seosd

In the [seosd] section, the tokens determine the behavior of the authorization daemon and the cache utility for performance improvement.

- **allow\_exec\_login** Recognizes the *exec login* shell script command as a login event.

**Values:** 0,1

**Default:** 0

- **autobypass\_level**

Specifies the level of automatic program bypass.

**Values:**

- disabled: auto-bypass is disabled
- info: Save information in the run-time table
- bypass: info + enable auto-bypass until next restart

**Default:** bypass

- **bypass\_filenames**

- Specifies a file that contains a list of file names to be exempted from seos events.

For example, `bypass_filenames = /opt/CA/PAMSC/bin/bypass_filenames`

**Default:** Token not set

- **bypass\_nfs\_port**

Specifies whether the port used by nfs (port 2049) are bypassed for CONNECT. The bypass exists to let NFS function correctly.

If you change the value of this token to *no*, there will be no bypass for this port. Make sure that you then provide the required Privileged Access Manager rules to replace this bypass. Following is an example of such rules (you *cannot* use them as is):

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
```

```
nr TCP 2049 owner(nobody) defaccess(none)
```

```
authorize TCP 2049 hostnet(all) access(w) uid(root)
```

```
nr TCP nfsd owner(nobody) defaccess(none)
```

```
authorize TCP nfsd hostnet(all) access(w) uid(root)
```

### NOTE

If you set the value of this token to *no* but do not provide the correct Privileged Access Manager rules, NFS stops working.

**Default:** yes

- **bypass\_outgoing\_TCPIP**

Defines a comma-separated list of ports for which seos\_syscall will not pass outgoing connection events to seosd.

**Default:** Token not set

- **bypass\_suid\_for\_login**

Specifies the path of the login program for which the dummy SUID system calls should be ignored.

This is used in case of some login programs, such as samba, which generate a large number of dummy SUID system calls. These system calls may interfere with the correct recognition of the logging in user.

**Default:** none

- **bypass\_suid\_program**

Allows multiple su commands. On some platforms, the system's su binary works in a nonstandard way: When an su command to a non-root user is requested, it executes su to root prior to executing su to the requested user.

If Privileged Access Manager surrogate protection is set for the root user, it may prevent the successful execution of an su to non-root users as well.

To use the surrogate protection for the root user on such platforms and still to be able to su to non-root users without interruption, set the bypass\_suid\_program token to contain the real path for the system's su binary.

**Default:** none

- **bypass\_system\_files**

Determines whether the Privileged Access Manager authorization engine should bypass read access for the /etc/passwd and /etc/group system files.

Valid values are:

**yes**-bypasses read access to system files.

**no**-does not bypass read access to system files.

**Default:** yes

- **bypass\_TCPIP**

Allows you to add one or more ports separated by commas for which seos\_syscall will not pass events to seosd.

The syntax is bypass\_TCPIP=*port1[,port2,portx]*

**Default:** Token not set

- **bypass\_whois** Defines utilities that the Privileged Access Manager bypasses.

**Values:** Utilities in *ACInstallDir/PAMSC/bin* **Default:** none

- **bypass\_xdm\_ports**

Specifies whether the ports used by xdm (ports 6000-6010) are bypassed for CONNECT. The bypass exists to let xdm function correctly.

If you change the value of this token to *no*, there will be no bypass for these ports. Make sure that you then provide the required Privileged Access Manager rules to replace this bypass. Following is an example of such rules (you *cannot* use them as is):

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)

nr TCP X-Win owner(nobody) defaccess(none)

authorize TCP X_Win hostnet(all) access(r)

authorize TCP X_Win hostnet(all) access(w) uid(root)

authorize TCP X_Win hostnet(all) access(w) gid(mygroup)

nr TCP 6000 owner(nobody) defaccess(none)

authorize TCP 6000 hostnet(all) access(r)
```



```
authorize TCP 6000 hostnet(all) access(w) uid(root)
```

```
authorize TCP 6000 hostnet(all) access(w) gid(mygroup)
```

### NOTE

If you set the value of this token to *no* but do not provide the correct Privileged Access Manager rules, xdm stops working. If the value of this token to *yes* and an outgoing connection is made via ports 6000-6010, the class name in the corresponding audit record is **TERMINAL**.

**Default:** yes

- **cron\_program**

Improves the check for cron login in seosd.

Set the cron\_program token to contain the real path for the system's cron binary.

**Default:** none

- **core\_if\_watchdog\_signal**

Specifies whether to create a core file when the watchdog process sends signal.

**Values:** yes, no

**Default:** no

- **dbdir**

Specifies the location of the Privileged Access Manager database.

**Default:** *ACInstallDir/seosdb*

- **debug\_backup\_dir**

Specifies the location of the backup debug files.

**Default:** Privileged Access Manager product log directory

- **debug\_backup\_num**

Defines the number of backup debug files to save.

**Values:** A positive number

**Default:** 2

- **debug\_file** Specifies the location of the seagent debug messages file.

**Default:** *ACInstallDir/log/seagent\_debug*

- **debug\_level**

Defines the lowest level of debug messages to save. The level of the value set and all levels above are saved.

**Values:** Disabled (no messages are saved), Critical, Very High, High, Normal., Low

**Default:** Critical

- **debug\_size**

Defines the maximum size in MBs of the debug messages file.

**Values:** A positive number

**Default:** 256

- **debug\_zone**

Defines which seosd submodules (zones) to produce debug messages for.

**Values:** -1 (All zones), 1 (SKI), 2 (QP), 4 (RESOLV), 8 (SEOSD), 10 (AUXFALLBACK), 20 (AUTH)

**Default:** -1

- **device\_file**

Specifies whether to scan all devices in /dev.

When the value of this token is set to Yes and the tty is not found in the standard list, Privileged Access Manager scans all the devices located in /dev.

(qplib resolves the tty name from the standard devices.)

### NOTE

You can add devices to the list of the tty names.

**Default:** no

- **dns\_server**

Specifies the DNS server name used to change host resolving from the default server to another server. This token is usually used when the DNS caching option is enabled.

**Default:** none

- **domain\_names**

Specifies a list of domain names that seosd appends to short host names it receives for authorization purposes in order to create a fully qualified name, so that these names can be authorized in the relevant HOST, CONNECT, or TERMINAL classes.

To identify a full name, seosd tries to append domain names in the domain\_names list to the short name for authorization purposes.

seosd first looks for a relevant rule in its database, using the short name only. If it does not find a record that matches the short name, it appends each domain name specified in the domain\_names token, one by one, until it finds a match.

For example, suppose you assign domain\_names the following list:

domain\_names= market.com, journey.com, total.com

Here is how seosd handles the matching process when a request from a subscriber called *acme*-which was not defined as a rule in the database-comes in:

acme (not found)acme.market.com (not found)acme.journey.com (not found)acme.total.com (found)

seosd uses the first record that matches (acme.total.com in this example) for authorization purposes.

**Default:** As defined in /etc/resolv.conf

- **EnablePolicyCache**

Determines whether a run-time table should be used to store the database values required for authorization. The run-time table is loaded to the memory when seosd starts. This avoids connecting to the database and thus reduces the authorization time.

Valid values are yes and no.

**Default:** no

- **FileCache\_auths**

If caching is enabled, specifies the number of records in the authorization pool. The maximum number of authorization records that can be cached is 800.

**Default:** 80

- **FileCache\_CleanInt**

Specifies how often to erase the file cache (in minutes).

**Default:** 60

- **FileCache\_files**

If caching is enabled, specifies the number of records in the file pool. The maximum number of file records that can be cached is 200.

**Default:** 20

- **FileCache\_InitPrio**

Specifies the initial priority value of new records in the cache table.

**Default:** 10

- **FileCache\_PriorInt**

If caching is enabled, specifies the frequency of recalculating priorities in the cache table. Each time a new record is saved counts as one.

**Default:** 1

- **FileCache\_users**

If caching is enabled, specifies the number of records in the user pool. The maximum number of user records that can be cached is 500.

**Default:** 50

- **ftp\_data\_port** Specifies the port number that ftp service uses to transfer data.

**Note:** Verify that the ftp\_data\_port number is identical in both seos.ini and /etc/services files. **Default:** 20

- **ftp\_port** Specifies the port number that ftp service uses to communicate.

**Note:** Verify that the ftp\_port number is identical in both seos.ini and /etc/services files. **Default:** 21

- **get\_login\_terminal**  
Determines whether seosd attempts to find the peer address of the login program in an alternative way. This is useful for connections such as ssh.  
Valid values include yes and no.  
**Default:** yes
- **grace\_admin**  
Determines the number of the grace logins that are set when an administrator changes users' passwords.  
**Default:** Token not set (1)
- **GroupidResolution**  
Determines how Privileged Access Manager resolves GID numbers to group names.  
Valid values include the following:  
**system**-Privileged Access Manager uses a system call to translate gid numbers. This value can be used for stand-alone, DNS client, and DNS server stations. (See also the resolve\_timeout token in this table.)  
**cache**-gid numbers and group names are cached in seosd. This is the fastest and easiest way to do translations but the cache cannot be updated during runtime.  
**ladb**-Privileged Access Manager uses a lookaside database to translate gid numbers. The sebuildla utility must be run to recreate the lookaside database each time an update to the relevant transaction table takes place.  
For NIS, and NIS+ servers, you can use either cache or ladb.  
For Sun Solaris 2.5 and above and HP-UX 11.x, you can use either cache or ladb.  
For all stations, the value ladb is preferred.  
**Default:** Token not set (system)
- **HostResolution**  
Determines how Privileged Access Manager resolves IP addresses to host names.  
Valid values include the following:  
**system**-Privileged Access Manager uses a system call to translate IP addresses. This value can be used for stand-alone, NIS/NIS+ client, and DNS client stations. (See also the resolve\_timeout token in this table.)  
**cache**-Host names and their IP addresses are cached in seosd. This is the fastest and easiest way to do translations but the cache cannot be updated during runtime.  
**ladb**-Privileged Access Manager uses a lookaside database to translate IP addresses. The sebuildla utility must be run to recreate the lookaside database each time an update to the relevant transaction table takes place.  
For NIS, NIS+, and DNS servers, you can use either cache or ladb; the value ladb is preferred.  
**Default:** Token not set (system)
- **IsolatedDaemon**  
Determines whether seosd closes the file descriptors stdin, stdout, and stderr when they become a daemon.  
Valid values include the following:  
**yes**-seosd closes these file descriptors when they become a daemon.  
**no**-seosd does not close these file descriptors when they become a daemon.  
**Default:** no
- **kill\_ignore**  
Specifies whether seosd ignores (denies) the kill -9 command directed toward any one of the three main Privileged Access Manager daemons. Valid values include the following:  
**yes**-Ignores the kill command. This is the default value.  
**no**-The kill command terminates seosd.  
**Default:** yes
- **login\_parent\_check**  
Specifies whether the parent process should continue (once a child process has logged in) with the login sequence or abandon the sequence and inherit the login from the child.  
Valid values are 0 and 1.  
If it is 0, the parent continues with the login sequence.  
If it is 1, the parent abandons the login sequence and inherits the login from the child.

**Default:** Token not set (0)

- **lookaside\_allowdupuid**

Determines whether sebuildla will register duplicate UIDs

Valid values:

**yes**-register duplicate UIDs

**no**-in case of duplicate UIDs, register only one UID

**NOTE**

Duplicate UIDs may cause inconstancy On UNIX OS

**Default:** no

- **lookaside\_path**

Specifies the directory where the lookaside database is located. Create this directory before running the sebuildla utility.

**Note:** The lookaside database files are built and updated using the sebuildla utility.

**Default:** *ACInstallDir/ladb*

- **max\_loggedin\_users**

Defines the maximum number of logged in users.

**Note:** This value determines the size of one of the internal memory tables. The larger the table, the more memory it consumes.

**Limits:** 4096-20480

**Default:** 8192

- **MultiLoginPgm**

Defines the name and full path of a program that performs multiple logins. It is used to detect the correct login sequence for these special login applications.

MultiLoginPgm is the login application name with the full path.

**Default:** none

- **network\_cache\_timeout**

Specifies the time interval, in minutes, between network cache-table cleanings, if network cache is used. Use this token to set time limits for the stored accepted incoming TCP requests.

**NOTE**

For more information about using the network cache, see the *Endpoint Administration Guide for UNIX*.

**Default:** 10

- **nfs\_devices**

Specifies the name and path of the file that contains the NFS major device numbers. Specify the full file path.

Privileged Access Manager uses this file if it fails to get the program using device and inode number and also fails to get it using its name. The file contains the NFS defaults for major device numbers for every platform. This may vary from system to system. To find the numbers for your system, use a small program with the UNIX getmajor() function. Then, edit the nfsdevs.init file (or the file you named with this token) to contain the numbers you find.

**NOTE**

Whenever you mount and remount the NFS system, you should update your nfsdevs.init file. You can also use the first four digits of the device only. These numbers remain unchanged, even when you unmount and remount the system.

**Default:** *ACInstallDir/etc/nfsdevs.init*

- **protect\_bin**

Specifies whether seosd protects the Privileged Access Manager binary files. Specify one of the following values:

**yes**-seosd protects the Privileged Access Manager binary files unless rules that allow such access are defined.

**NOTE**

Do not specify yes when the \_default access for your FILE records is none because, unless all /opt/CA/PAMSC/bin files have FILE records, inaccessibility of files could make Privileged Access Manager unusable.

**no-seosd** does not protect the Privileged Access Manager binary files.

**Default:** no

- **resolve\_rebind**

Specifies if seosd re-establishes the connection to the NIS server after a time-out failure.

We strongly recommend that you do not change the default value.

**Default:** yes

- **resolve\_timeout**

Specifies the maximum number of seconds seosd tries to resolve IP to address, user ID to user name, group ID to group name, or service port number to service name.

The value takes effect in two cases:

When seosd is using system resolution. (See the HostResolution, ServiceResolution, UseridResolution, and GroupidResolution tokens.)

When the under \_NIS\_server token is set to no.

If the specified time expires without a resolution, seosd assumes that no resolution exists for the specified IP, ID, or port.

If value is set to 0, there is no time out.

**Default:** 5

- **rt\_priority**

Determines whether seosd has real-time priority.

Valid values are yes and no

When this token is set to yes, seosd will have real-time priority.

**Default:** yes

- **ServiceResolution**

Determines how Privileged Access Manager translates TCP port numbers to service names.

Valid values include the following:

**system**-Privileged Access Manager uses a system call to translate TCP port numbers. This value can be used for stand-alone, NIS/NIS+ client, DNS client, and DNS server stations. (See also the resolve\_timeout token in this table.)

**cache**-Service names and their TCP port numbers are cached in seosd. This is the fastest and easiest way to do translations but the cache cannot be updated during runtime.

**ladb**-Privileged Access Manager uses a lookaside database to translate TCP port numbers. The sebuildla utility must be run to recreate the lookaside database each time an update to the relevant transaction table takes place.

For NIS, and NIS+ servers, use either cache or ladb.

**Default:** system

- **sim\_login\_timeout**

Defines the timeout (in minutes) before Privileged Access Manager removes unused simulated login user entries from the Accessor Element Entry table (ACEE).

Privileged Access Manager performs a simulated login to create ACEE entries when it needs access to information that can be found in the ACEE.

**Default:** 60

- **special\_check**

Specifies whether to enable file path checking on kernel module loading. When enabled, Privileged Access Manager checks that the kernel module to be loaded matches the filepath property of the KMODULE record (for non-Linux systems), or matches the signature of the KMODULE record (for Linux systems).

**Default:** no

- **terminal\_default\_ignore**

Determines whether the defaccess value of the \_default TERMINAL and of the specific TERMINAL records are considered when authorizing administrative access.

Valid values are yes and no.

**yes**-Administrative access ignores the defaccess value of the \_default and of any specific TERMINAL records. In this case, administrative access will require an explicit authorization rule for a relevant specific TERMINAL record.

**no-** Administrative access considers the defaccess value of all relevant TERMINAL records whether it is `_default` or specific.

**Default:** yes

- **terminal\_search\_order**

Specifies whether seosd tries to check a TERMINAL defined by name before trying it by its IP address.

Valid values are:

**name** - TERMINALs will be checked by name before IP address.

**ip** - TERMINALs will be checked by IP address before name.

**NOTE**

TERMINAL class supports generic rules defined by wildcards (IP address or host name pattern match). Generic rules are *always* checked after specific (full-name) rules. For example, if you set this to *ip*, seosd looks for a TERMINAL resource in the following order: complete IP address match, complete host name match, IP address pattern match, host name pattern match.

**Default:** name

- **trace\_backup** Specifies whether to back up the trace messages file when it reaches the configured file size limit.

**Values:** yes, no

When set to yes, the `trace_backup` token saves a backup of the trace file, and creates a trace file.

**Default:** yes

- **trace\_file\_backup** Specifies the location of the trace messages backup file.

**Default:** *ACInstallDir/log/seosd.trace.bak*

- **trace\_file**

Specifies the name of the file to which the trace messages are sent, if trace messages are requested.

**Default:** *ACInstallDir/log/seosd.trace*

- **trace\_file\_size** Defines the maximum size of the trace messages file.

**Default:** 512 MB

- **trace\_file\_type**

Determines whether the trace file is written in binary or text format.

Valid values include the following:

**binary**-The trace file should be written in binary format. This option reduces the space occupied by this file.

**text**-The trace file should be written in text format.

The daemon seosd checks the value of this token and compares it to the contents of the trace file. If the token value does not match the format of the trace file, seosd saves the trace file under its name and adds the extension `.backup`.

**Default:** text

- **trace\_filter**

Specifies the name and path of the file that contains the filter data that is used to filter the trace messages.

**Default:** *ACInstallDir/data/language/etc/trcfilter.init*

- **trace\_space\_saver**

Specifies the amount of free space, in MB, to be left in the file system. When the amount of free space is less than this number, Privileged Access Manager disables the trace.

**NOTE**

Trace is never automatically enabled, even if more space becomes available at a later time.

**Default:** 512

- **trace\_to**

Specifies the destination of trace messages.

Valid values include the following:

**file**-Privileged Access Manager sends the trace messages to the file specified by the `trace_file` token. To disable tracing, use the `secons -t` command. For more information, see the `trace_file` token in this table.

**file,stop**-Privileged Access Manager generates trace messages during daemon initialization. Once the daemon is initialized, trace messages generation stops.

**none**-Privileged Access Manager does not issue trace messages. This is the normal setting after you install and implement Privileged Access Manager.

**NOTE**

If the token is set to **file** or **file,stop**, the Privileged Access Manager trace can be toggled with the **seosd** command with the **-t** option.

**Default:** file, stop

- **update\_dev\_trusted\_pgm** Specifies whether **seosd** updates the trusted program device number when the trusted program starts.  
**Values:** yes, no  
**Default:** yes
- **UpdSurrogLogin**  
Specifies whether Privileged Access Manager updates the user's last access time on a surrogate login.  
Valid values are:  
**1** - Privileged Access Manager updates the user's last access time on a surrogate login.  
**0** - Privileged Access Manager does *not* update the user's last access time on a surrogate login
- **Undef\_ForPacI**  
Determines whether **seosd** checks an undefined user when there is an asterisk (\*) in the accessor's name in a PACL.  
Valid values include the following:  
**1**-**seosd** will not include undefined users with an asterisk in their PACL.  
**0**-**seosd** will include undefined users with an asterisk in their PACL.  
**Default:** 0
- **under\_NIS\_server**  
Determines whether **seosd** uses internal name resolution instead of system name resolution.  
Valid values include the following:  
**yes**-**seosd** stores in memory or in a lookaside database (see the **use\_lookaside** token) all user, group, host, and port information during startup.  
This is required for NIS, NIS+, and DNS server machines, and for the following operating systems: Sun Solaris 2.5 and above, HP-UX 11.x, IBM AIX 4.3.x, and IRIX 6.5.

**WARNING**

Turning this token off could hang the machine if it is an NIS server or one of the previously-mentioned operating systems.

**no-seosd** uses system name resolution and the **resolve\_timeout** token takes effect.

**NOTE**

This token is automatically assigned a value during installation.

This token remains for purposes of backward compatibility only. If you have a new Privileged Access Manager installation or an installation of version 2 or higher, use the tokens **HostResolution**, **ServiceResolution**, **UseridResolution**, and **GroupidResolution** instead.

**Default:** Assigned during installation

- **use\_lookaside**  
Determines whether **seosd** stores the user, group, host, and port information in a lookaside database or in memory.

**NOTE**

This token is used in conjunction with the **under\_NIS\_server** token and has no relevance unless the **under\_NIS\_server** token is set to **yes**.

Valid values include the following:

**yes**-**seosd** uses the lookaside database for user, group, host, and service details. The lookaside database is built by the **sebuildla** utility and can be refreshed by it at any time.

The location of the lookaside database is set by the **lookaside\_path** token.

**no-seosd** caches all user, group, host, and service information during startup so that all translations can be done in memory. We recommend that seosd be restarted daily to refresh the cache.

This token remains for purposes of backward compatibility only. If you have a new Privileged Access Manager installation or an installation of version 2 or higher, use the tokens HostResolution, ServiceResolution, UseridResolution, and GroupidResolution instead.

**Default:** no

- **use\_mapped\_user\_name**

(Valid if both Privileged Access Manager and UNAB are installed) Specifies whether seosd uses the user enterprise name in audit records.

**Values:** yes, no

**Default:** no

- **use\_nfs\_devices**

Determines whether to use NFS devices. Valid values are yes or no.

**Default:** Yes

- **use\_standard\_functions**

Determines whether sebuildla in an NIS environment will retrieve users by calling the standard system function getpwent or by parsing the output of ypcat passwd and cat /etc/passwd commands.

Valid values are:

**yes**-use the standard system function getpwent

**no**-use parsing of the output of ypcat passwd and cat /etc/passwd commands.

**Default:** yes

- **use\_trusted\_script**

Specifies whether seosd will use the trusted script mechanism.

When the trusted script mechanism is used, programs called from within a shell script retain the name of the shell script in the internal Privileged Access Manager tables.

This means that if a script was used in a PACL, these programs will inherit that privilege. This also means that you cannot protect these programs via Privileged Access Manager.

A trusted script begins with #! on the first line.

When the trusted script mechanism is **not** used, these programs will be registered in the internal Privileged Access Manager tables under their own names.

**Default:** yes

- **use\_unab\_db**

(Valid if both Privileged Access Manager and UNAB are installed) Specifies whether seosd uses the UNAB database to resolve users and groups name if the current method is unable to do so. This token coincides with the tokens: use\_lookaside, UseridResolution, GroupidResolution.

**Values:** yes, no

**Default:** no

- **UseFileCache**

Specifies whether to use the cache tool for file records to improve performance.

**Default:** yes

- **UseNetworkCache**

Determines whether Privileged Access Manager caches accepted incoming TCP requests.

#### **NOTE**

For more information about using the network cache, see the *Endpoint Administration Guide for UNIX*.

Valid values are yes and no.

**Default:** no

- **UseridResolution**

Specifies how Privileged Access Manager translates UID numbers to user names.

Valid values include the following:

**system**-Privileged Access Manager uses a system call to translate uid numbers. This value can be used for stand-alone, NIS/NIS+ client, DNS client, and DNS server stations.



**cache**-User names and their uid numbers are cached in seosd. This is the fastest and easiest way to do translations but the cache cannot be updated during runtime.

**ladb**-Privileged Access Manager uses a lookaside database to translate uid numbers. The sebuildla utility must be run to recreate the lookaside database each time an update to the relevant transaction table takes place.

For NIS and NIS+ servers, Sun Solaris 2.5 and above, or HP-UX 11.x operating systems, you must use either cache or ladb.

**Default:** system

- **watchdog\_refresh**

Determines whether seosd refreshes the Watchdog to scan the privileged programs and secured files for each file handle.

Valid values include the following:

**yes**-seosd refreshes the Watchdog.

**no**-seosd does not refresh the Watchdog.

**Default:** no

## seosdb

In the [seosdb] section, the tokens manage database checking and rebuilding.

- **CheckAlways**

Determines whether the database should be checked for corruption at Privileged Access Manager initialization.

Valid values are yes and no.

**Default:** yes

- **CheckProgram**

Specifies the full path and parameters of an alternative command to be used instead of the internal code for checking the database. The command should return 0 if the database is valid or a nonzero number if it should be corrected.

**Default:** Token not set (do not run any program; same as using *dbmgr -u -fast*)

- **CreateNewClasses**

Specifies whether you can add new classes, created with the seclassadm utility, to a database.

Valid values are yes and no.

**Default:** yes

- **CreateNewProps**

Specifies whether to save data about the new properties in a file when the Privileged Access Manager sepropadm utility creates new database property.

Valid values are yes and no.

If it is yes, sepropadm saves the data about new properties in a file and when dbmgr -c utility later generates the new Privileged Access Manager database, dbmgr uses this file to add these properties to the database.

**Default:** yes

- **RebuildAlways**

Indicates whether the Privileged Access Manager database should always be rebuilt at Privileged Access Manager initialization.

Valid values are yes and no.

**Default:** no

- **RebuildProgram**

Specifies the full path and parameters of an alternative command to be used instead of the internal code for correcting the database.

**Default:** Token not set (do not run any program; same as using *dbmgr -u -build all*)

## seoswd (UNIX)

In the [seoswd] section, the tokens determine the behavior of the Watchdog.

**agent\_manager\_check\_enabled**

Specifies whether to protect the AgentManager daemon.

**Default:** no

**agent\_manager\_refresh\_interval**

Specifies the interval when the Watchdog checks if the Agent Manager daemon is running or not.

**Default:** 10 minutes

**BlockingInterval**

Specifies the interval, in seconds, that the Watchdog waits for a response from the main daemon. When elapsed, the Watchdog sends a signal to the main daemon.

**Default:** 60 seconds

**debug\_backup\_dir**

Defines the location of the backup debug messages files.

**Default:** Privileged Access Manager product log directory

**debug\_backup\_num**

Defines the number of debug backup files to save.

**Values:** A positive number

**Default:** 2

**debug\_file**

Defines the location of the file to which seoswd debug messages are written.

**Default:** /log/seoswd\_debug under the CM product directory

**debug\_level**

Defines the lowest level of debug messages to save. The level of the value set and all levels above are saved.

**Values:** Disabled (no messages are saved), Critical, Very High, High, Normal, Low

**Default:** Critical

**debug\_size**

Defines the maximum size in MBs of the debug messages file.

**Values:** A positive number

**Default:** 256

**IgnoreScanInterval**

Specifies whether to scan programs and files at specific intervals.

If the token value is no, then the Watchdog performs interval scanning. If the value is yes, then it does not scan at intervals.

**NOTE**

If you do not specify the scan times with the PgmTestTime or SecFileTestTime tokens, and this token is set to yes, then the Watchdog does not scan trusted programs or secured files respectively.

**Default:** no

**PgmRest**

Specifies the period, in seconds, after the last event and before checking programs again. The program rests to prevent system overload.

**Default:** 10 seconds

### **PgmTestInterval**

Specifies the time interval, in seconds, between the rescanning of trusted programs.

#### **NOTE**

If the value equals or is greater than one day (86400 seconds), then IgnoreScanInterval defaults to yes.

**Default:** 18000 seconds (five hours)

### **PgmTestStartTime**

Specifies the start time, in hh:mm format, of the first trusted program scan.

**Default:** If you do not set this token, the Watchdog performs the first scan shortly after startup.

### **PgmTestTime**

Specifies fixed scan times, in hh:mm format, for trusted programs. You can specify more than one scan time by separating them with spaces.

**Default:** If you do not specify scan times, and you set the IgnoreScanInterval token to yes, then the Watchdog does not scan trusted programs.

### **policyfetcher\_refresh\_interval**

Specifies the interval, in seconds, to verify that the policyfetcher daemon is running.

**Default:** 600

### **ProcHandlesCritical**

Specifies the process critical handle count. The Watchdog restarts the process when the critical handle count is exceeded.

**Valid Values:** 0 (disables token), 800 (minimum value)

**Default Value:** 1500

### **ProcHandlesHigh**

Specifies the high watermark for the process handle count. The Watchdog restarts the process during the restart hours when the defined handle count is exceeded.

**Valid Values:** 0 (disables token), 800 (minimum value)

#### **NOTE**

The token is disabled if the value is greater than ProcHandlesCritical value.

**Default Value:** 1000

### **ProcRestartHours**

Specifies the hours when the Watchdog restarts the high handle count process.

**Valid Values:** 0 - 23 (value in hours)

**Default Value:** 0 - 5

### **ProcVSizeCritical**

Specifies the process critical memory size in megabytes. The Watchdog restarts the process immediately when the specified limit is exceeded.

**Default Value:** 500 MB

### **ProcVSizeHigh**

Specifies the high watermark for process memory size. The Watchdog restarts during the restart hours.

**Default Value:** 300 (value in megabytes)

### **ProcVSizeInterval**

Specifies the interval, in seconds, between the process performance counters verification. The Watchdog checks the following processes:

SeOS Watchdog (seoswd)  
 SeOS Engine (seosd)  
 SeOS Agent (SeOSAgent)  
 SeOS Policy Model (sepmdd)  
 CA ControlMinder Agent Manager (AgentManager)  
 CA ControlMinder Report Agent (ReportAgent)  
 Default: 900 seconds

### **RefreshParams**

Specifies the time interval, in seconds, between successive reads by the Watchdog of the seos.ini tokens.

**Default:** 86400 (one day)

### **SecFileRest**

Specifies the period, in seconds, after the last event and before checking secured files again. To prevent system overload, the Watchdog rests.

#### **NOTE**

If you do not specify scan times, and you set the IgnoreScanInterval token to yes, then seoswd does not scan secured files.

**Default:** 10

### **SecFileTestInterval**

Specifies the time interval, in seconds, between the rescanning of secured files.

**Default:** 36000 (ten hours)

### **SecFileTestStartTime**

Specifies the start time, in hh:mm format, of the first scan of secured files.

**Default:** If no value is given, the Watchdog performs the first scan a short time after the Privileged Access Manager daemons start.

### **SecFileTestTime**

Specifies fixed scan times, in hh:mm format, for secured files. You can specify more than one scan time by separating them with spaces.

**Default:** N/A

### **SeosAYT**

(UNIX only) Specifies the time interval, in seconds, between the Watchdog checks of the daemon seosd ("Are you there?").

#### **WARNING**

Do not modify this token by yourself because an incorrect value can cause problems in the operation of Privileged Access Manager. For assistance, contact CA Support at <http://ca.com/support>.

**Default:** 60

**SignalMinInterval**

Specifies the interval, in seconds, between scans after a HUP signal triggers a one-time scan on demand, to protect the system against overload.

**NOTE**

Scan on demand is performed both on trusted programs and secured files.

**Default:** 60

**UnTrustMissing**

Determines whether the Watchdog attempts to untrust a program or file, even though it cannot find it. For example, if the file was deleted or the relevant NFS partition is not mounted.

**Values:** yes (Attempt to untrust the missing file), no (Do not attempt to untrust the missing file).

**Default:** yes

**unab\_check\_enabled**

Specifies whether to protect the authentication daemon.

**Values:** yes, no

**Default:** no

**unab\_refresh\_interval**

Specifies the interval, in seconds, to verify that the authentication daemon is running.

**Default:** 600

**UnTrustMissing**

Specifies whether the Watchdog must attempt to untrust a program or a file, even though it is not found. For example, a file is deleted or the relevant NFS partition is not mounted.

**Values:** yes (attempt to untrust the missing file), no (do not attempt to untrust the missing file)

**Default:** yes

**VerifyCtime**

Specifies whether Privileged Access Manager Watchdog checks the time of the last file status change of trusted programs and secure files.

**Valid Values:** yes, no.

**Default:** no

**WatchdogRequestsInterfaceName**

Specifies the pipe server name which communicates with the Watchdog.

**Default:** WatchdogRequests

**serevu**

In the [serevu] section, the tokens determine the attributes of the serevu utility.

- **config\_file**

Specifies the location of the serevu configuration file.

**Default:** *ACInstallDir/etc/serevu.cfg*

- **def\_diff\_time**

Specifies the time interval during which serevu scans the relevant system log for failed logins.

The value can be specified in seconds (that is, 300) or minutes (that is, 5m).

For example, if the token is set to 300, serevu searches for failed logins that occurred during the previous 300 seconds.

We recommend that this value be an even multiple of the value in the *def\_sleep\_time* token.

**Default:** 5m (5 minutes)

- **def\_disable\_time**

Specifies the time that a user account is disabled because of too many failed login attempts.

The value can be specified in seconds (that is, 300) or minutes (that is, 5m). You can also use the *FOREVER* value to disable user logins forever.

**WARNING**

Use the *FOREVER* value to disable user logins permanently.

**Default:** 6m (6 minutes)

- **def\_fail\_count**

Specifies the number of failed logins each user is entitled to, per period, in the token *def\_diff\_time*.

Users with at least this number of failed logins over the specified time period are disabled.

**NOTE**

We recommend that the number of failed logins always be the same as the value of allowed unsuccessful login attempts set on your system. For example, on Sun Solaris use the *RETRIES* token in the */etc/default/login* file to set the system value.

Default values are five for Solaris and three for HP-UX and AIX. See your operating system documentation for more details.

**Default:** 5

- **def\_sleep\_time**

Specifies the time between successive serevu checks.

The value can be specified in seconds (that is, 120) or minutes (that is, 2m).

**Default:** 2m (2 minutes)

- **save\_disable\_path**

Specifies the location of the disabled user accounts list so serevu can handle disabled users when it goes down.

**Default:** *ACInstallDir/log/serevu\_disable.users*

## sesu

In the [sesu] section, the tokens control logging on as a user other than yourself, without having to enter the password of the other user.

- **AlwaysTargetShell**

Determines whether to use the target shell (SysV style) or the invoker shell (BSD style). If yes, Privileged Access Manager uses the target user shell.

Valid values are yes and no.

**Default:** no

- **FilterEnv**

Specifies a list of environment variables that sesu does not pass to the shell when the target user is root. Separate variable names with spaces or tabs.

No default.

- **old\_sesu**

Determines whether the old or new sesu utility is used.

Valid values include the following:

**yes**-Use the old `sesu` utility as it was in previous versions.

**no**-The new `sesu` utility calls the native `su` program (as defined in the `SystemSu` token) to ensure consistency between `su` and `sesu`. If the `SystemSu` token is not valid, `sesu` reverts to the old mechanism.

**NOTE**

If this token is set to `no`, the tokens `Path`, `AlwaysTargetShell`, `sys_env_file`, and `FilterEnv` are ignored.

**Default:** yes

- **Path**

Specifies the value that `sesu` uses to set the `PATH` environment variable. If the token is not set, `sesu` does not set the `PATH` variable.

No default.

- **request\_target\_password**

Specifies whether to request the password of the target user when the `old_sesu` token is set to `no` and the user is executing `sesu` for a non-root user.

**Default:** yes

- **UseStrongAuthentication**

Specifies whether `sesu` requests the users to strongly authenticate themselves by providing a One Time Password.

**Note:** Define the authentication server in the `strong_auth_server` token of the `strong_auth` section.

**Valid values:** yes, no

**Default:** no

- **sys\_env\_file**

Specifies an ASCII file containing environment variable values for the `sesu` session. This token is relevant only when starting `sesu` with the `-` parameter (`sesu -`). The format for each line of the file is *variable = value*.

**Default:** None (except for IBM AIX where it is `/etc/environment`)

- **SystemSu**

Specifies the location of the `/bin/su` program. Update this token if you use a program in a location other than the default location. When `sesu` cannot find the authorization daemon, it executes the program specified in this token.

**NOTE**

On AIX, replace the system `su` binary with a symbolic link to the `sesu` wrapper instead of the `sesu` binary.

**Default:** `/bin/su`

- **UseInvokerPassword**

Determines whether `sesu` requires the invokers to specify their own passwords. If the token value is `no`, `sesu` does not require any password.

**Default:** no

## sesudo

In the `[sesudo]` section, the tokens determine the attributes of the `sesudo` utility.

- **echo\_command**

Determines whether `sesudo` displays the command before executing it. To echo the command, set the token value to `yes`.

**Default:** No

- **echo\_success**

Determines whether `sesudo` should print the successful message to the terminal when a successful `sesudo` command is run.

Valid values are `yes` and `no`.

**Default:** yes

## standalone1

In the [standalone] section, the tokens specify options for administrating using a standalone machine.

- **full\_login\_check**  
Specifies whether to consider administrating a site using standalone as a login.  
**Valid values:** 0 and 1. When this token is set to 1, it is considered as a login to the machine.  
**Default:** 0

## strong\_auth

In the [strong\_auth] section, the tokens define the strong authentication server.

**Note:** For more information about how to set up strong authentication, see the CA AuthMinder topic in the *Privileged Access Manager Integration* section.

- **strong\_auth\_server**  
Defines the URL of the strong authentication server used by the sepromote utility.  
**Example:** (for SSL connection) ssl://123.456.7.89:9742  
**Example:** (for non SSL connection) tcp://otp\_server.com:7222  
**Default:** none
- **organization\_name**  
Defines the organization where CA Strong Authentication searches users of strong authentication. Sepromote users can overwrite the value of this token from the command line.  
**Note:** For more information about this CA Strong Authentication parameter, see the Setting the Default Organization section in the *CA Strong Authentication Administration Guide*.  
**Default:** "defaultorg"

## tcp\_communication

In the [tcp\_communication] section, the token defines common TCP connection settings.

- **listening\_backlog**  
Defines the number of simultaneous new TCP connection requests that each listening block can establish.  
**Default:** 128

## The UNAB Conflicts File

The UNAB conflicts file is created after you attempt to migrate users and group to Active Directory. The file details the conflicts that were discovered by UNAB during the migration process. Review this file to resolve the conflicts that are reported in the file.

This file contains the following fields:

```
Solution Entity Type,Solution Entity Name,Solution Operation,Solution AD Mapped Name,Conflicts,UID,Home
Directory,GID,Member of,Members,GECOS
```

- **Solution Entity Type**  
Displays the type of solution entity to migrate.  
**Limits:** user, group
- **Solution Entity Name**  
Displays the name of the entity.
- **Solution Operation**  
Displays the entity migration status.



**Limits:** Keeplocal, Migrate, Map

- **Solution AD Mapped Name**  
Displays the Active Directory account name that the local account is mapped to.
- **Conflicts**  
Displays the conflicts that were found during the migration.
- **UID**  
Displays the user ID.
- **Home Directory**  
Displays the user home directory.
- **GID**  
Displays the group ID.
- **Member Of**  
Displays the groups that the user is a member of.
- **Members**  
Displays a list of users that are members in the group.
- **GECOS**  
Displays GECOS information.

## The uxauth.ini File

### Valid on UNIX

The uxauth.ini configuration file contains various tokens that control the functionality of UNAB. The UNAB configuration file is divided into sections that relate to different sets of tokens that control UNAB functionality:

Section	Description
ad	Contains Active Directory tokens with the parameters that you entered during installation
agent	Contains tokens that control the various UNAB parameters
global	Contains tokens that control UNAB general settings
libdefaults	Contains tokens that control Kerberos configuration settings
logmgr	Contains tokens that the UNAB logging utility uses
map	Contains tokens that specify Active Directory attribute names
message	Contains tokens that UNAB uses to define the message file
migrate	Contains tokens that UNAB uses during the migration process
nss_cache_update_post_job	Specifies the UNAB utility that was used to prepare an input file to drive post-updates of the UNAB nss.db database by the UNAB agent. Post-update utilities can be found in the UNAB libin subdirectory. Available options: postupdate-nss-gr Default value: none nss_cache_update_post_job = none
one way trust	Contains tokens that UNAB uses to support one way trust domains
pam	Contains tokens that control the UNAB PAM module
passwd	Contains tokens that UNAB uses to control password changes during the migration process
register	Contains tokens that control the UNAB registration functionality

## ad

The [ad] section contains Active Directory tokens with the parameters that you entered during installation.

- **ad\_domain**  
Defines the name of the Active Directory domain.  
  
**NOTE**  
Do not manually edit the value of this configuration setting. Use the uxconsole -register utility to set the value of this configuration setting.
- **ad\_gc\_port**  
Specifies the port that the Active Directory Global Catalog service uses.  
**Default:** 3268
- **ad\_site**  
Defines the name of the Active Directory site that contains the DCs that the UNIX host uses to communicate with Active Directory.  
Any values in the lookup\_dc\_list override the value of this configuration setting. The UNIX host does not communicate with any DC listed in the ignore\_dc\_list configuration setting.  
  
**NOTE**  
Do not manually edit the value of this configuration setting. Use the uxconsole -register utility to set the value of this configuration setting.  
  
**Default:** none
- **base\_dn**  
Defines the base\_dn of the Active Directory server. Privileged Access Manager automatically sets the value of this configuration setting.
- **cache\_cleanup\_interval**  
Specifies the cleanup interval, in hours to clean up the local users and group cache for users that are removed from partner domains with one-way trust with the registered domain. This parameter is ignored if the registration domain has no partners with one-way trust.  
**Value:** Any positive integer.  
**Default:** 24  
**Example:** cache\_cleanup\_interval = 24
- **cache\_cleanup\_startup\_time**  
Specifies the start time to clean up the local users and group cache for users that are removed from partner domains with one-way trust with the registered domain. This parameter is ignored if the registration domain has no partners with one-way trust.  
**Value:** Any integer from 0 through 23.  
**Default:** 3 (cleanup starts at 3am)  
**Example:** cache\_cleanup\_startup\_time = 3
- **computer\_container**  
Defines the location of the UNIX host in Active Directory.  
**Default:** cn=Computers
- **domain\_query\_order**  
Specifies the order in which UNAB queries Active Directory domains for users and groups.  
**Options:** none-no order specified; comma separated list of Active Directory domains  
**Default:** none
- **group\_container**  
Specifies the base entry to search for UNIX users in Active Directory.  
**Limits:** container name (cn=groups), ROOT for the complete Active Directory query.  
**Default:** ROOT
- **group\_custom\_filter**  
Specifies a custom search filter to apply during groups search in Active Directory.

**Example:** gidNumber=\*

**Default:** none

- **ignore\_dc\_list**  
Specifies the Active Directory domain controllers that are ignored for LDAP connection.  
**Options:** none, comma separated list of fully qualified host names  
**Default:** none
- **ignore\_domain\_list**  
Specifies the Active Directory domains that UNAB ignores when it queries users and groups.  
**Options:** none - query current and all trusted domains; all - do not query trusted domains; a comma separated list of domains to ignore.  
**Default:** none
- **ignore\_group\_container**  
Specifies the Active Directory group containers to ignore. Containers are defined by their Distinguished Names, comma separated.  
**Limits:** none, comma separated list of distinguished names  
**Default:** none
- **ignore\_user\_container**  
Specifies the Active Directory user containers to ignore. Containers are defined by their Distinguished Names, comma separated.  
**Limits:** none, comma separated list of distinguished names  
**Default:** none
- **ldap\_port**  
Defines the port the Active Directory LDAP service uses.  
**Default:** 389
- **lookup\_dc\_list**  
Specifies the Active Directory domain controllers that are used for LDAP connection. If you specify a list of domain controllers, UNAB uses the specified domain controllers only. If you do not specify the DCs to use, UNAB discovers the Active Directory site that is closest to the physical location of the endpoint and communicates with DCs in the discovered site.  
**Options:** none, comma separated list of fully qualified host names.  
**Default:** none
- **lookup\_domain\_list**  
Specifies the Active Directory domains that established a bi-directional trust with the domain that you registered UNAB.  
**Options:** none, UNAB automatically discovers the trusted domains, comma separated list of trusted domains  
**Default:** none
- **user\_container**  
Specifies the base entry to search for UNIX users in Active Directory.  
**Limits:** container name, ROOT for complete Active Directory query.  
**Default:** ROOT
- **user\_custom\_filter**  
Specifies a custom search filter to apply during users search in Active Directory.  
**Default:** none

## agent

Privileged Access Manager maintains agent settings it uses under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Agent

Agent key entries (and any subkeys) are for internal use only.

- **ShutdownWaitingTimeout**

Defines the timeout period, in milliseconds, the Privileged Access Manager Agent waits for its components to gracefully shut down. If Privileged Access Manager components do not shut down gracefully, the Agent shuts down forcefully.

**Note:** This registry entry is for internal use only.

**Default:** 60000

## global (uxauth.ini)

The [global] section contains the parameters that control the UNAB general settings.

- **activation**  
Specifies the host activation level.  
**Limits:** 0, 1, 2
  - 0 - not registered
  - 1 - registered (login permitted for user defined in local user store only)
  - 2 - activated (login is permitted for users who are defined in local user store or defined in either the .allow file or in the UNAB login policy)**Default:** 0
- **CASHCOMP**  
Specifies the path to the CA shared components install directory.  
**Default:** /opt/CA/SharedComponents
- **integration\_mode**  
Specifies the UNAB installation method.  
**Limits:** 1 - partial integration, 2 - full integration  
**Note:** Specify partial integration (1) if you want to maintain the UNIX user store.  
**Default:** 2
- **locale**  
Defines the language for the UNAB agent and utilities.  
**Example:** C (English), japanese, chinese-s, chinese-t  
**Default:** C
- **kerberos\_configuration**  
Specifies how Kerberos configuration is used when implementing a UNAB assisted Kerberos SSO.  
**Limits:**
  - internal Specifies that the configuration file and user credential caches are stored under /opt/CA/uxauth and opt/CA/uxauth/etc directories
  - external Specifies that the configuration file and user credential caches are stored in their native locations

**NOTE**  
This token is automatically configured during UNAB registration. Linux, HPUX, and Solaris store the user credentials in /tmp directory. AIX stores the user credentials in /var/krb5/security/creds directory

**Default:** internal
- **product\_path**  
Defines the name of the UNAB install directory.  
**Default:** /opt/CA/uxauth

## libdefaults

The [libdefaults] section contains tokens that control Kerberos configuration settings.

- **default\_realm**

Defines the default Kerberos realm for the UNAB endpoint. A value of *unregistered* specifies that UNAB does not use Kerberos.

**Default:** unregistered

- **dns\_lookup\_kdc**

Specifies that UNAB uses DNS SRV (service locator) records to look up the KDC (Key Distribution Centre) services location.

**Limits:** true, false

**Default:** true

- **dns\_lookup\_realm**

Specifies that UNAB uses DNS TXT records to look up domain to realm mappings.

**Limits:** true, false

**Default:** false

- **ticket\_lifetime**

Defines the ticket lifetime in seconds.

**Default:** 2400

## logmgr (uxauth.ini)

The [logmgr] section contains tokens that the UNAB logging utility uses.

- **audit\_back**

Defines the full path name of the audit log backup file.

**Default:** /opt/CA/uxauth/log/uxauth.audit.bak

- **audit\_group**

Specifies the name of the group that is permitted to read the audit log files.

**Limits:** none, *group\_name*

– None - No group access, only root can read the audit log files

– *group\_name* - Defines the name of the group that can read the audit log files

### NOTE

If you change the value of this token after UNAB creates the audit log file, you must use *selang* commands to set the file group ownership and the group permissions to read the log. Any files that are created after you set the value of this token have the permissions that you specify.

**Default:** none

- **audit\_log**

Defines the full path name of the audit log file.

**Default:** /opt/CA/uxauth/log/uxauth.audit

- **audit\_max\_files**

Defines the maximum number of audit log files to save for each of the specified backup modes. When the maximum number of backup audit log files is reached, UNAB deletes the oldest backup file when it creates the newest. A value of 0 specifies that UNAB keeps accumulating backup files.

**Default:** 0

- **audit\_size**

Defines the maximum size of the audit log file in KB.

**Note:** The minimum value that you can specify for this token is 50 KB.

**Default:** 1024

- **audit\_to\_syslog**

Specifies whether to log audit events to syslog file.

**Limits:** yes, no

**Default:** no

- **BackUp\_Date**

Specifies the interval for backing up the audit log files.

**Limits:** none, yes, daily, weekly, monthly

- none - performs the backup when the file reaches the size that is specified in the audit\_size token but does not timestamp the file.
- yes - Audit log file backup is performed when the audit file reaches the size that is specified in the audit\_size token
- daily - Audit log files backup is performed daily
- weekly - Audit log files backup is performed on a weekly basis
- monthly - Audit log files backup is performed on a monthly basis

**Note:** If you specify daily, weekly, or monthly for this token, UNAB creates a time stamp, backs up the audit log file when the current date surpasses the specified interval, and appends the time stamp to the name of the backup file. However, if the size of the audit log file reaches the size that is specified in the audit\_size token before the current date surpasses the specified interval, UNAB backs up the audit log. UNAB does not append the time stamp to the name of the backup file. If you specify yes for this token, the time stamp is always appended to the name of the backup file.

**Default:** none

- **error\_back**

Defines the full path name of the error log file backup copy.

**Default:** /opt/CA/uxauth/log/uxauth.error.bak

- **error\_group**

Specifies the name of the group that is permitted to read the error log files.

**Limits:** none, *group\_name*

- None - No group access, only root can read the error log files
- *group\_name* - Defines the name of the group that can read the error log files

**Note:** If you change the value of this token after UNAB creates the error log file, you must use `selang` commands to set the file group ownership and the group permissions to read the log. Any files that are created after you set the value of this token have the permissions that you specify.

**Default:** none

- **error\_log**

Defines the full path name of the error log file.

**Default:** /opt/CA/uxauth/log/uxauth.error

- **error\_size**

Specifies the maximum size of the error log file in KB.

**Note:** The minimum value that you can specify for this token is 50 KB.

**Default:** 50

## map

### Valid in Full Integration Mode

The [map] section contains tokens that UNAB uses to specify Active Directory attribute names.

- **group\_gid\_attr\_name**

Specifies the Active Directory attribute name that indicates the UNIX group ID.

**Default:** gidNimber

- **group\_member\_attr\_name**

Specifies the Active Directory attribute name that lists members of a group.

**Limits:** member, memberUid

**Note:** Use value memberUid only when user\_name\_attr\_name = msSFU30Name.

**Default:** member

- **user\_gecos\_attr\_name**

Specifies the Active Directory attribute name that indicates the UNIX user gecos.

**Default:** gecoss

- **user\_gid\_attr\_name**  
Specifies the Active Directory attribute name that indicates the UNIX group ID.  
**Default:** gidNumber
- **user\_homedir\_attr\_name**  
Specifies the Active Directory attribute name that indicates the UNIX user home directory.  
**Default:** unixHomeDirectory
- **user\_loginshell\_attr\_name**  
Specifies the Active Directory attribute name that indicates the UNIX user login shell.  
**Default:** loginShell
- **user\_name\_attr\_name**  
Specifies the Active Directory attribute name for the UNIX user name.  
**Default:** sAMAccountName
- **user\_uid\_attr\_name**  
Specifies the Active Directory attribute name that indicates the UNIX user ID.  
**Default:** uidNumber

## message (uxauth.ini)

The [message] section contains tokens UNAB uses to define the message file.

- **filename**  
Defines the full path name of the message file.  
**Default:** /opt/CA/uxauth/data/uxauth.msg

## migrate

The [migrate] section contains tokens that UNAB uses during the migration process.

- **conflicts\_file**  
Defines the full path name of the migration conflicts file.  
**Default:** /opt/CA/uxauth/log/migrate.conflicts
- **create\_ad\_groups**  
Specifies whether to create new Active Directory groups during migration if no identical groups were found in Active Directory.  
**Limits:** yes, no  
**Default:** yes
- **disable\_mapped\_user**  
Specifies whether to disable the UNIX password of partially migrated (mapped) users.  
**Limits:** yes, no  
**Default:** yes
- **ignore\_gecos\_conflict**  
Defines whether to ignore gecoss user attribute-related conflicts that UNAB finds during the migration process.  
**Limits:** yes, no  
**Default:** yes
- **is\_gid\_migration\_a\_prerequisite**  
Specifies whether the migration of the user's primary group is a prerequisite to migrate the user.  
**Limits:** yes, no  
**Default:** no
- **journal**  
Defines the full path name of the migration journal file.

**Default:** /opt/CA/uxauth/log/migrate.journal

- **minimal\_gid**  
Defines the minimal group ID that will be migrated to Active Directory during the migration process. Groups with a lesser GID are not migrated.  
**Default:** 101
- **minimal\_uid**  
Defines the minimal user ID that will be migrated to Active Directory during the migration process. Users with a lesser UID are not migrated.  
**Default:** 101
- **remove\_migrated\_user**  
Specifies whether to remove the local user account after migration.  
**Limits:** yes, no  
**Default:** yes
- **try\_to\_map\_on\_conflict**  
Specifies whether to map conflicting accounts if the full migration process fails.  
**Limits:** yes, no  
**Default:** yes

## passwd (uxauth.ini)

The [passwd] section contains tokens that UNAB uses to control password changes during the migration process.

- **YpGrpCmd**  
Defines the command to generate the NIS group map.  
**Default:** make group
- **YpMakeDir**  
Defines the makefile directory that is used when creating NIS maps.  
**Default:** /var/yp
- **YpPassCmd**  
Defines the command to generate the NIS password map.  
**Default:** make passwd
- **YpServerGroup**  
Defines the full pathname of the group file on the NIS server.  
**Default:** /etc/group
- **YpServerPasswd**  
Defines the full pathname of the password file on the NIS server.  
**Default:** /etc/passwd
- **YpServerSecure**  
Defines the full pathname to the password file of the operating system.  
**Default (AIX):** /etc/security/passwd  
**Default (HP-UX):** /.secure/etc/passwd  
**Default (Solaris):** /etc/shadow  
**Default (all other OS):** /etc/shadow

## one\_way\_trust

The [one\_way\_trust] section contains tokens that UNAB uses to manage one-way trust domains.

### NOTE

For each domain UNAB maintains a separate entry in this section.

- **domains**



Specifies the Active Directory domains that have a one-way trust relationship with the UNAB registration domain.

**Options:** a comma separated list of domains, none

**Default:** none

### Example: One-way trust domain entry

The following example shows how UNAB maintains a one-way trust domain details:

```
[domain.company.com]
ep_name=Computer
ep_type=Windows Agentless
account_name=Administrator
account_container=Accounts
```

In this example, you have established a one-way trust with the domain (domain.company.com) and specified the endpoint type (Windows Agentless), domain user account that is used to retrieve users and groups details from the domain (Administrator) and the account container in Active Directory domain (Accounts).

#### NOTE

You do not have to specify an administrator account. The user account must have permissions to read users and groups attributes only.

## pam

The [pam] section contains tokens that UNAB uses to interact with the PAM module.

- **debug\_mode\_for\_user**  
Defines whether the PAM module can print messages to the user screen during login.  
**Options:** yes, no  
**Default:** yes
- **home\_directory\_permission**  
Specifies the default file permissions that are assigned to the user home directory.  
**Values:** 0-7  
**Default:** 700  
**Example:** 700 indicates that each user has read, write, and execute permissions to their home directories only.
- **pam\_ad\_password\_only**  
Defines the PAM module behavior when the mapped user logs in with a local password.  
**Options:** yes, no  
**Default:** yes
- **pam\_delete\_user\_ccache**  
Defines whether the pam\_uxauth module deletes the Active Directory user credentials cache upon login completion.  
**Values:** Yes (Delete the AD user credentials after login), no (The credentials cache is not changed)  
**Default:** No
- **pam\_exit\_on\_deny**  
Defines the PAM module behavior if the login was denied due to enterprise or local policy settings or Active Directory account state.  
**Options:** yes (The PAM module closes the sequence and prevents other PAM modules from authenticating the user), no (The PAM module does not close and enables other PAM modules to authenticate the user. The no value allows the login server to retry the PAM sequence call)  
**Default:** yes
- **pam\_receive\_timeout**  
Specifies the time, in seconds, that the PAM module waits for the UNAB agent (uxauthd) to respond.  
**Limits:** any positive integer.

**Default:** 10

- **user\_minimal\_uid**

Defines the minimal UID for the local storage to authenticate in the Active Directory.

**Values:** any positive number.

**Default:** 101

## register

The [register] section contains tokens that control UNAB registration functionality.

- **start\_uxauthd**

Specifies whether to run the uxactivate utility at the end of the installation process.

**Limits:** yes, no

**Default:** yes

- **verbose**

Defines the verbose level to use during the installation process.

**Default:** 0

## trcfilter.init

### Valid on UNIX

The Privileged Access Manager daemon also uses the trcfilter.init initialization file.

This optional file contains entries that specify filter masks for filtering out Privileged Access Manager trace messages. Each line of the file contains a regular expression. When a message is sent to the trace file, seosd checks whether the message matches one of the entries in the trcfilter.init file. It writes the trace message to the file only if it does not match any of the expressions specified in the trcfilter.init file.

For example, the following trcfilter.init file causes all messages that begin with INFO or WATCHDOG to be discarded. They are not written to the trace file.

```
WATCHDOG*
```

```
INFO*
```

### NOTE

This file does not filter audit records generated by user traces. To filter these audit records, edit the audit.cfg file.

## Utilities

### acuxchkey Utility: Change Encryption Key Settings

Use the acuxchkey utility to change encryption key and Message Queue settings. This command has the following format:

```
acuxchkey -t -pwd password
```

- **-t**

Specifies the Message Queue change option.

- **-pwd *password***

Defines the Message Queue password.

### Example: Change Message Queue Password

This command saves the changed Message Queue encrypted password in the database. The password is "secret", and must be in clear text and enclosed in double quotes:

```
acuxchkey -t -pwd "secret"
```

### Example: Change Distribution Server Communication Settings

This example shows you how to change the Distribution Server settings to work with SSL:

```
env config
editres CONFIG accommon.ini section (communication) token (Distribution_Server) value ("ssl://DS_host:61616")
```

## ChangeEncryptionMethod Utility: Change Encryption Method

### Valid on UNIX

The ChangeEncryptionMethod utility changes the encryption methods.

#### NOTE

This utility is supplied as a script file and is located in the lbin directory.

When you run this utility, you can select one of the following encryption methods:

- DEFAULT
- AES (128bit, 192bit, or 256bit)
- DES
- TRIPLEDES
- SCRAMBLE

If you do not specify an encryption method, the utility prompts you for it. The utility searches for existing Policy Models in the system. The utility then decrypts them by running "sepm -de pmd\_name", and changes the encryption method by linking libcrypt to the new shared library: libaes128, libaes192, libaes256, libdes, libtripledes, or libscramble.

#### NOTE

To run this utility, Privileged Access Manager must be running. To change the encryption method, the script asks you whether it can temporarily shut down Privileged Access Manager.

#### WARNING

Verify that you use identical encryption methods on the Privileged Access Manager Enterprise Management server and on the Privileged Access Manager endpoints. All password history is lost if you select to change the encryption method of existing endpoints.

This command has the following format:

```
ChangeEncryptionMethod.sh [DES|TRIPLEDES|SCRAMBLE|AES128|AES192|AES256]
```

## dbmgr Utility

The dbmgr utility lets you create, manage, and maintain the Privileged Access Manager database files.

#### NOTE

This utility replaces the following utilities from previous versions: dbdump, rdbdump, dbutil, secreddb, sedb2scr, and semigrate.

**Important!** Use this utility only with the guidance of support personnel during problem resolution. For assistance, contact CA Support at <http://ca.com/support>.

To run the dbmgr utility, you must have the ADMIN, AUDITOR, or SERVER attribute.

The utility handles several tasks and has the associated following functions:

Task	Function
Create a database	dbmgr -create
Display database information	dbmgr -dump
Create a script that defines a database	dbmgr -export
Copy database data to a flat file	dbmgr -migrate
Manage an existing database	dbmgr -util
Backup a database	dbmgr -backup
Restore a database	dbmgr -restore

### dbmgr -create Function: Create a Database

The dbmgr -create function generates a new empty database. Use this function only at installation time, or when you want to create a database or PMDB. Privileged Access Manager creates the database in the current directory.

#### NOTE

If you want to add user-defined classes to the new database, first run the seclassadm utility after creating the new database.

This command has the following format:

```
dbmgr {-create|-c} {-c[q]|-h} [-d] [-f filename] \
[-n] [-o] [-t terminalNames] \
[-u userName [,userName...]] [-ux userName [,userName...]] \
[-v] [-w] [-k] [-n pathName]
```

- **-create|-c**  
Executes the database creation function of the dbmgr utility.
- **-c**  
Prompts you for whether you want to create a new database.
- **-cq**  
Creates a new database without prompting you first.
- **-h**  
Displays the help for this function.
- **-d**  
Prints database layout documentation. The output contains a full description of the structure and property formats used in the database.
- **-f filename**  
Defines a file to direct output to, instead of the standard output device.
- **-k**  
Specifies to run the coexistence utility when the database creation completes.
- **-n pathName**  
(UNIX Only). Defines the full pathname of the Privileged Access Manager database to back up.  
When you are creating a new database, a basic class scheme is generated. When you are adding new classes to the database using the seclassadm utility, the class information is stored in a file in the database directory. To back up a specific database with its class scheme (such as a policy model database), specify its location with the -n option. The user-defined class information is taken from that location. If you do not specify the -n option, the class information file

is searched for in the local directory where the database is to be created. If it is not found there, the file is taken from the active Privileged Access Manager security database directory.

- **-t *terminalName***  
Defines a comma-separated list of terminals, from which the superusers can manage the local database, to create in the database.
- **-u *userName* [*userName...*]**  
Defines a comma-separated list of users to create in the database. These users are defined as Privileged Access Manager security administrators.  
If the -t option is specified, these users are authorized to manage the local database from the defined terminals.  
See also the -ux parameter.
- **-xu *userName* [*userName...*]**  
Defines a comma-separated list of enterprise users to be defined as Privileged Access Manager security administrators.  
If the -t option is specified, these users are authorized to manage the local database from the defined terminals.  
If no users are created dbmgr -create creates a user in the database that corresponds to *root* on UNIX, or Administrator on Windows, with the ADMIN, AUDITOR, and IGN\_HOL attributes.
- **-v**  
Disables the progress messages.

#### NOTE

The -v and -d options cannot be used together.

#### Example: Create a new database on Windows

If at the system prompt `c:\temp>`, enter the following command:

```
dbmgr -c -c -u user1 -t myterminal.company.com
```

When you confirm that you want to create the database, the utility creates a new database in the `c:\temp` directory. It creates the user *user1* in the database, who has the ADMIN, AUDITOR, and IGN\_HOL attributes, and can administer the database from the terminal *myterminal.company.com*.

#### Example: Create a new database on UNIX

If at the `\tmp\db` directory, enter the following command:

```
dbmgr -c -cq -d -f dbLayout
```

The utility creates a new database in the `\tmp\db` directory. It also creates a file (*dbLayout*) that contains the database layout documentation. By default, it creates the user *root* in the database, and assigns it the ADMIN, AUDITOR, and IGN\_HOL attributes.

#### dbmgr -dump Function: Display Database Information

The `dbmgr -dump` function reports on the records in the database. Use this function to perform the following operations:

- Display information for records of a specified class
- Display information for a single record of a specified class
- Display information for all records of a class, except a specified one
- Generate lists of classes and property definitions
- Generate a list of groups that a user belongs to
- Generate a list of records of a particular class

This function assumes that the Privileged Access Manager daemons are not running; you must invoke it from the directory where the database resides. If you use the -r switch, Privileged Access Manager daemons must be running, and you

must have the ADMIN, AUDITOR, or SERVER attribute. To execute this function, you must also have READ and WRITE permission on the database files.

This command has the following format:

```
dbmgr {-dump|-d} [-h] [-r] [-f fileName] \
[c] [fc] [g user] [l class] [p class] [fp class] \
[d class [props|@fileName] \
[dn class [props|@fileName] \
[e classrecord [props|@fileName] \
[en classrecord [props|@fileName] \
[o classrecord [props|@fileName] \
[on classrecord [props|@fileName]
```

- **-dump|-d**  
Executes the database dump function of the dbmgr utility.
- **-f *fileName***  
Directs output to the specified file, instead of the standard output device.
- **-h**  
Displays the help for this function.
- **-r**  
Displays information about the database currently being used by the authorization daemon.  
If you omit this option, dbmgr displays information about the database in the current directory.
- **c**  
Lists the names of all classes defined in the database.
- **d *class* [*props*|@*fileName*]**  
Displays the values of selected properties for all records of a class. The *class* parameter specifies the class. The *props* parameter defines a space-separated list of properties whose values you want to display.  
To read the property list from a file, specify the full pathname of a file, preceded by an at sign (@). Each property listed in the file must appear on a separate line.  
If you do not specify any properties, the values of all the properties are listed.
- **dn *class* [*props*|@*fileName*]**  
Same as the *d* option, only properties with unknown values are not displayed.
- **e *class record* [*props*|@*fileName*]**  
Displays the values of selected properties for all records of a class *except* for a single, specified record. The *class* parameter specifies the class. The *record* parameter specifies the name of the record to omit from the list. The *props* parameter defines a space-separated list of properties whose values you want to display.  
To read the property list from a file, specify the full pathname of a file, preceded by an at sign (@). Each property listed in the file must appear on a separate line.  
If you do not specify any properties, the values of all the properties are listed.
- **en *class record* [*props*|@*fileName*]**  
Same as the *e* option, only properties with unknown values are not displayed.
- **fc**  
Lists all class information for all classes in the database.
- **fp *class***  
Lists all property information on properties of the specified class.
- **g *user***  
Lists the groups that the specified user is a member of.
- **l *class***  
Lists all the records in the specified class.
- **o *class record property* / on *class record property***

Displays the values of selected properties for a single record of a class. The *class* parameter specifies the class. The *record* parameter specifies the record. The *props* parameter defines a space-separated list of properties whose values you want to display.

To read the property list from a file, specify the full pathname of a file, preceded by an at sign (@). Each property listed in the file must appear on a separate line.

If you do not specify any properties, the values of all the properties are listed.

- *o class record property / on class record property*  
Same as the *o* option, only properties with unknown values are not displayed.
- *p class*  
Lists the names of the properties of the specified class.

#### NOTE

You can only specify one other option apart from *-r* and *-f*.

## dbmgr -export Function: Create Script that Defines a Database

The *dbmgr -export* function replicates a database on other stations. It generates a script that consists of the *selang* commands required to define an existing database.

#### NOTE

You cannot copy database files from one architecture to another when using native commands (such as *cp* or *tar* on UNIX or *copy* on Windows), if the files do not use the same byte order. For example, you cannot copy a database from a Sparc-based machine to an Intel based machine, because each uses a different byte order.

#### WARNING

Review the script before you execute it.

This command has the following format:

```
dbmgr {-export|-e} {-l|-r} [-c className] [-f fileName]
```

- **-export|-e**  
Executes the database export function of the *dbmgr* utility.
- **-h**  
Displays the help for this function.
- **-l**  
Exports the database in the current directory.

#### NOTE

This option assumes the Privileged Access Manager daemons are not running. If the daemons are running, then it assumes you are operating on a different database from the one being used by the daemons.

- **-r**  
Exports the database currently being used by Privileged Access Manager. You must have the *ADMIN* or *SERVER* attribute, and the Privileged Access Manager daemons must be running.
- **-c className**  
Defines a space-separated list of classes which you want to export from the database.
- **-f fileName**  
Directs output to the specified file, instead of the standard output device. You can then create a new database from the file, by instructing *selang* to read the commands from the file.

## dbmgr -migrate Function to Copy Data to a Flat File

The dbmgr -migrate function copies data from user and program records in an existing database to a flat file (binary format). The function can also copy the data from the flat file into a new database. The database from which the data is imported must be version 1.21 or later.

When you copy a flat file into a new database, use the same version of this function that you used to create the flat file. If you have more than one version, we strongly recommend that you use the most recent version.

**Note:** For better security, delete the old database, the script that is used to build the new database, and the flat file created by this function after copying the data from the old database into the new database.

### WARNING

Always create a backup of the database before using this function.

This command has the following format:

```
dbmgr {migrate|-m} {-r|-w|-h} [-s] filename \

[-v versionNumber] [-f fileName]
```

- **-migrate|-m**  
Executes the database migration function of the dbmgr utility.
- **filename**  
Defines the flat file that you want to copy data from or into.
- **-f filename**  
Directs output to the specified file, instead of the standard output device.
- **-h**  
Displays the help for this function.
- **-r**  
Reads the database in the current directory and copies certain data into the flat file *filename*.
- **-s**  
Reads the information from the database using the Privileged Access Manager server rather than reading the database directly. This option is only valid with the -r switch.  
You must have administrator privileges and R (read) and W (write) access to the terminal to use this option.  
If you do not specify this option, the function reads from or writes to the database in the current directory.
- **-v versionNumber**  
Reads a flat file that was created by a previous version. This option is only valid for -w command. Enter this option after the file name and supply the version number.
- **-w**  
Reads the flat file *filename* and copies the data into the database in the current directory.

### Example: Copy data from an existing database to a new database

The following steps illustrate how to copy data from an existing database into a new database. The old database is assumed to be in the directory /tmp/old\_db. The new database is assumed to be in the directory *ACInstallDir*/seosdb (where *ACInstallDir* is the directory in which you installed Privileged Access Manager).

**Note:** This procedure is written using UNIX pathnames but can be followed on Windows by modifying these pathnames as appropriate.

#### Follow these steps:

1. Log in as a superuser.



2. If the product daemons are running, shut them down with the following command:

```
secons -s
```

3. Create a backup of the old database by copying it to a different location or to a backup medium.
4. Copy the database into /tmp/old\_db, then create a script that duplicates the old database by running the dbmgr utility on the old database:

```
cd /tmp/old_db

/opt/CA/PAMSC/bin/dbmgr -export -l -f lang_script
```

5. Create a database:

```
cd /opt/CA/PAMSC/seosdb

/opt/CA/PAMSC/bin/dbmgr -c -cq
```

6. Execute the script that is generated in the previous step and create the database:

```
cd /opt/CA/PAMSC/seosdb

/opt/CA/PAMSC/bin/selang -l /tmp/old_db/lang_script
```

7. Execute the dbmgr utility to create a flat file containing data from the old database:

```
cd /tmp/old_db

/opt/CA/PAMSC/bin/dbmgr -migrate -r flat_file
```

8. Load the data from the flat file into the new database:

```
cd /opt/CA/PAMSC/seosdb

/opt/CA/PAMSC/bin/dbmgr -migrate -w /tmp/old_db/flat_file
```

## dbmgr -util Function: Manage Existing Database

The dbmgr -util function performs management and maintenance operations on a database. It assumes Privileged Access Manager is not currently running. Invoke it from the directory where the database resides.

The -util option is used to manage and manipulate the local database specified by the parameter *filename*. Database files have the extension .dat and must be DBIO files. Database index files (files with the extension .001) cannot be used with the -util option.

This command has the following format:

```
dbmgr {-util|-u} [-h] \
[-all filename] \
```

```

[-build filename] \
[-check] \
[-close] \
[-dump filename] \
[-dup srcdst] \
[-fast] \
[-free filename] \
[-index filename] \
[-key filename] \
[-load dbascii] \
[-scan filename] \
[-scana filename] \
[-stat filename] \
[-verify] \
[-f fileName]

```

- **-util-u**  
Executes the database management and maintenance functions of the dbmgr utility.
- **-all *filename***  
Performs all index checks; same as specifying the *-index* and *-free* options.
- **-build *filename***  
Builds indexes of a DBIO based on data records.
- **-check**  
(UNIX only). Performs a fast sanity and consistency check on all index entries for all database files.
- **-close**  
Closes the database if it is open.
- **-dump *filename***  
Dumps the data file as ASCII on the standard output device.
- **-dup *src dst***  
Duplicates the DBIO file based on the file header.
- **-f *fileName***  
Directs output to the specified file, instead of the standard output device.
- **-fast**  
Performs a fast sanity check on all index entries for all the database files.
- **-free *filename***  
Checks for a free index.
- **-index *filename***  
Checks the consistency of the index.
- **-key *filename***  
Sequentially scans an index file.
- **-load *db* ascii**  
Loads an ASCII file and converts it into a DBIO file.
- **-scan *filename***  
Scans the database sequentially.
- **-scana *filename***  
Scans the database sequentially, including deleted records.
- **-stat *filename***  
Lists the header information of the database file.
- **-verify**  
(UNIX only). Verifies that certain predefined objects exist in the database; for example, SEOS, ADMIN, and UACC for all classes.

## dbmgr -backup Function: Back Up a Database

The dbmgr -backup function creates an online backup of the Privileged Access Manager database in the specified directory. This function is available whether the Privileged Access Manager daemons are running or not.

This command has the following format:

```
dbmgr {-backup|-b} backup_directory
```

- **-backup|-b**  
Executes the database backup function of the dbmgr utility.
- *backup\_directory*  
Defines the backup directory. This directory cannot be located on a remote machine; if the directory does not exist, the function creates it.

## dbmgr -restore Function: Restore a Database

### Valid on UNIX

The dbmgr -restore function performs an online restore of the Privileged Access Manager database in the specified directory. This function is available whether the Privileged Access Manager daemons are running or not.

This command has the following format:

```
dbmgr {-restore|-r} restore_directory
```

- **-restore|-r**  
Executes the database restore function of the dbmgr utility.
- *restore\_directory*  
Defines the directory where the database you want to restore resides.

## DictImport Utility: Import the Dictionary File

The DictImport utility prepares and imports dictionary files into the Privileged Access Manager database. After you install Privileged Access Manager, import the dictionary file into the product database and then activate it. You can then set password protection.

The DictImport utility sets the use\_dbdict password rule to *db* and activates the DICTIONARY class and PASSWORD class.

### NOTE

The centralized dictionary is disabled if the PASSWORD class is not active.

This command has the following format:

```
DictImport [-h] [-o selangFilename] [-f dictionaryFilename]
```

### NOTE

This utility is supplied as a script file and is located in the lbin directory.

- **-f dictionaryFilename**  
Generates selang commands that import all the dictionary words from the specified file. If you omit this option, the dictionary file is defined from values in the configuration settings.
- **-h**  
Displays the help for this utility.
- **-o selangFilename**  
Writes selang commands to the specified file. If you omit this option, selang commands are written to the standard output device.

## dmsmgr Utility

The dmsmgr utility lets you manage the advanced policy management infrastructure. Infrastructure components include Privileged Access Manager endpoints, Deployment Map Server (DMS), and Distribution Host (DH).

The utility handles several tasks and has the associated following functions:

Task	Function
Create a DMS or a DH	dmsmgr -create
Remove a DMS or a DH	dmsmgr -remove
Remove obsolete nodes from the DMS database	dmsmgr -cleanup
Configure advanced policy management	dmsmgr -config
Restore a DMS or a DH	dmsmgr -restore
Synchronize a DMS or an HD	dmsmgr -sync

### dmsmgr -create Function: Create a DMS or a DH

The dmsmgr -create function creates a Deployment Map Server (DMS) or a Distribution Host (DH) on a computer where Privileged Access Manager is installed.

#### NOTE

You can also create a DMS or a DH during installation.

#### NOTE

The user running the utility is always granted administration rights for the created DMS or DH.

This command has the following format:

```
dmsmgr -create -auto [-osgroups] [-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts]
dmsmgr -create -dms name \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts] [-subscriber dh-names]
dmsmgr -create -dh name \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts]
```

- **-admin *user* [,user...]]**  
(Optional) Defines internal users as administrators of the created DMS or DH.
- **-auto**  
Creates a DMS and a DH with default names (DMS\_\_, DH\_\_, and DH\_\_WRITER).  
Use this option to create a DMS and a DH and the required associations between them.
- **-osgroups**  
(Optional) Specifies to create predefined host groups when you create a DMS.
- **-desktop *hosts***  
(Optional) Defines a comma-separated list of computers that have TERMINAL access rights to the computer with the created DMS or DH.

#### NOTE

Whether specified or not, the terminal running the utility is always granted administration rights for the created DMS or DH.

- **-dh *name***

Creates a DH with the *name* specified on the local host.

#### NOTE

If you use this option to create a DH, Privileged Access Manager tells you to synchronize the DMS and DH even if the DH is already subscribed and no policies were previously sent. This message is a reminder of the steps you need to take and may not be indicative of the actual situation. If you completed all required steps, you can safely ignore it.

- **-dms *name***  
Creates a DMS with the *name* specified on the local host.
- **-subscriber *dh\_names***  
(Optional) Defines a comma-separated list of DH PMDBs that the created DMS will policy updates to. Specify each DH in the following format: *DH\_name@hostname*.
- **-xadmin *user* [,*user*...]**  
(Optional) Defines enterprise users as administrators of the created DMS or DH.

### dmsmgr -remove Function: Remove a DMS or a DH

The dmsmgr -remove function removes a DMS or a DH on a computer where Privileged Access Manager is installed.

This command has the following format:

```
dmsmgr -remove {-dms|dh} name
dmsmgr -remove -auto
```

- **-auto**  
Removes the default DMS and DH from the local host.  
These are the DMS and DH databases created by default during installation or when you use dmsmgr -create -auto.
- **-dh *name***  
Removes the specified *name* DH from the local host.
- **-dms *name***  
Removes the specified *name* DMS from the local host.

### dmsmgr -cleanup Function: Remove Obsolete Nodes

The dmsmgr -cleanup function removes obsolete nodes from the DMS or DH database. These are HNODE objects that represent Privileged Access Manager nodes that have been unavailable for a specified amount of time.

#### NOTE

As a routine maintenance procedure, clean the DMS and DH from these obsolete nodes.

This command has the following formats:

```
dmsmgr -cleanup {-hnode|-deployment} -days number {-dms|-dh} name
dmsmgr -cleanup -policy name -vcount number {-dms|dh} name
```

- **-hnode**  
Removes HNODE objects that represent Privileged Access Manager nodes that have been unavailable for more than *number* days.
- **-deployment**  
Removes the DEPLOYMENT objects that are older than *number* days.
- **-policy *name***  
Removes the POLICY objects (policy versions) that belong to the specified policy and are older than *number* versions.
- **-dh *name***

- Defines the name of the DH you want to remove the obsolete nodes from.
- **-dms *name***  
Defines the name of the DMS you want to remove the obsolete nodes from.
- **-vcount**  
Defines the number of versions to keep.

## dmsmgr -config Function: Configure Advanced Policy Management

The dmsmgr -config function configures advanced policy management.

This command has the following format:

```
dmsmgr -config[-] [host_name] {-endpoint|-dhname names|-drname names}
dmsmgr -config -osgroups [-dms name]
```

- **-config[-]**  
Configures or removes the configuration of advanced policy management.
- **-dhname *names***  
Configures the endpoint to work with the comma-separated list of Distribution Hosts.
- **-dms *name***  
Defines the name of the DMS on which the automatic host groups are created.
- **-drname *names***  
Configures the endpoint to work with the comma-separated list of disaster recovery Distribution Hosts.
- **-endpoint**  
Configures the endpoint for advanced policy management.
- ***host\_name***  
Performs the configuration on *host\_name*. If no host is specified, performs the configuration on the local computer.
- **-osgroups**  
Adds automatic host groups to the DMS.  
**Note:** For more information about automatic host groups, see the *Enterprise Administration Guide*.

## dmsmgr -restore Function Restore a DMS or DH

The dmsmgr -restore function restores a DMS or a DH from backup files. You can restore a DMS or DH when Privileged Access Manager is running or stopped, over an existing DMS, or into a new directory.

This command has the following format:

```
dmsmgr -restore -dms name -source path\
[-replica name] [-subscriber dhname[,dhname...]] \
[-admin user[,user...]] [-xadmin user[,user...]]
dmsmgr -restore -dh name -source path\
[-admin user[,user...]] \
[-xadmin user[,user...]] [-desktop host[,host...]]
```

- **-admin *user[,user...]***  
(UNIX) Defines internal users as administrators of the restored DMS or DH.
- **-desktop *host[, host...]***  
(Optional) Defines a list of computers that have TERMINAL access rights to the computer with the restored DH.

### NOTE

Whether specified or not, the terminal running the utility is always granted administration rights for the restored DH.

- **-dh *name***

Defines the name of the DH that is restored on the local host.

- **-dms *name***  
Defines the name of the DMS that is restored on the local host.
- **-replica *name***  
(Optional) Defines the name of the disaster recovery DMS. Use this parameter if you have set up Privileged Access Manager in a disaster recovery deployment and restore a production DMS. Specify the disaster recovery DMS name in the following format: *DMS\_name@hostname*.
- **-source *path***  
Defines the directory that contains the backup files to restore.
- **-subscriber *dh\_name*[, *dh\_name*...]**  
(Optional) Defines a comma-separated list of DHs that the restored DMS sends policy updates to. Specify each DH in the following format: *DH\_name@hostname*.
- **-xadmin *user*[,*user*...]**  
(UNIX) Defines enterprise users as administrators of the restored DMS or DH.

## **dmsmgr -sync Function Synchronize a DMS or a DH**

The dmsmgr -sync function synchronizes between the DMS and the DH to create a mirror image of the DMS on the DH. You can execute the synchronization process from the Enterprise Management Server or from a dedicated Distribution Server.

This command has the following format:

```
dmsmgr -sync -dhname <dhname> [-dms<dms-name>]
```

```
dmsmgr -sync self [-dh<dhname>]
```

- **-dms<dms-name>**  
Synchronizes the DMS with the DH.

### **NOTE**

Run the command from the DMS computer.

- **-dh<dhname>**  
Synchronizes the DH with the DMS.

### **NOTE**

Run the command from the DH computer.

- **-dhname<name>**  
Specifies a comma separated list of Distribution Hosts.
- **self**  
Specifies to synchronize the DH with the DMS.

### **NOTE**

Run the command from the Distribution Server.

## **eACoexist Utility Detect and Register Coexisting Trusted Programs**

### **Valid on Windows**

The eACoexist utility detects any coexisting programs in the local system (for example, CA Anti-Virus). If the detected program is trusted, Privileged Access Manager registers the program using a SPECIALPGM rule. A special program rule defines the types of access for that program and makes sure that Privileged Access Manager bypasses it when granting access.

This command has the following format:

eACoexist [plug-in-path]

- *plug-in-path*  
(Optional) Defines the path to the folder that contains the coexistence plug-ins you want the coexistence program to use.  
If you do not define a path, the program uses the default path where the coexistence plug-ins are stored (*ACInstallDir\Coexistence*).

## The Coexistence Utility

The coexistence utility (eACoexist) that Privileged Access Manager supplies, lets you resolve potential conflicts with other programs on the local computer.

When the coexistence utility runs, it performs the following actions:

1. Checks that *one* of the following conditions apply:
  - a. Privileged Access Manager is not running.
  - b. You have the ADMIN attribute.
 If neither conditions apply, the utility exits.
2. Locates the response.ini file, as follows:
  - When the utility runs during installation, it uses the path *media\_drive:\Coexistence\\_architecture*
  - If Privileged Access Manager is installed on the computer, it uses the following registry key value:  
`HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSD\ResponseFile`
 If the file does not exist the utility exits.
3. Locates the coexistence plug-ins directory, as follows:
  - If you run the utility and pass a parameter from the command line, it uses this parameter as the path of the plug-in.
  - When the utility runs during installation, it uses the path *media\_drive:\Coexistence\\_architecture*
  - If you run the utility with no parameters, it concatenates the string "Coexistence" to the following registry key value:  
`HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSPath`
 If the directory does not exist, or there are no coexistence plug-ins in the directory, the utility exits.
4. Executes the discovery process.  
To do this, it enumerates the executables in the coexistence plug-ins directory and executes them one by one, as follows:
  - a. Stores the result of the plug-in execution in %windir%\EACDiscovery.ini

### NOTE

The utility automatically deletes this file on successful completion of the plug-in discovery process.

- b. Checks that the output file EACDiscovery.ini exists.  
If the file does not exist, the utility continues to execute the next plug-in.
- c. For each product section in EACDiscovery.ini, concatenates the section (product) name and version value and checks whether the response file contains the matching section.

### NOTE

The response.ini file contains a section for each coexisting program. If a section name appears with a version number, for example, eTrust Audit-1.5, the utility performs the action only for the specified version.

- d. If a matching section exists in the response file, executes the action that is set by the value of the Act-Utility-0 in that section, as follows:
  - Issues a warning that the discovered product is not compatible with Privileged Access Manager.
  - Stops the discovered services of the product.



The utility retrieves the discovered services of the product from the EACDiscovery.ini file.

- Same as bullet 2, but during Privileged Access Manager installation.
- Starts the services if the discovered product.

The utility retrieves the services of the discovered product from the EACDiscovery.ini file.

- Creates trusted program rules (SPECIALPGM) for the processes of the discovered product and starts Privileged Access Manager.

The utility retrieves the processes of the discovered product from the EACDiscovery.ini file. It also retrieves the respective program type (pgmtype) from this file. It then creates a temporary script file (*ACInstallDir\Data\discoveryscp*) that it executes when Privileged Access Manager starts.

- Same as bullet 2, but during Privileged Access Manager uninstall.

#### NOTE

Each section can contain more than one action. For example, you can have Act-Utility-0, Act-Utility-1, and Act-Utility-2 that are executed in that order.

### Policy Manager Plug-In

The coexistence utility runs the Policy Manager plug-in to scan the computer for Policy Manager registry keys and executables before the Privileged Access Manager installation begins, as follows:

- Queries the following registry key for existence:

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\SeAM.Exe`

If the registry key exists, the plug-in:

- Reads the value of the Path entry
- Returns the following executable pathname:

`FilePathFromRegistry\Bin\SeAM.exe`

- Issues a compatibility warning during Privileged Access Manager installation

This is the default action as defined in the response file. The Policy Manager plug-in does not add a trusted program (SPECIALPGM) rule by default.

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on). Also, the Policy Manager application is no longer provided with Privileged Access Manager.

### BrightStor Plug-In

The coexistence utility runs the BrightStor plug-in to scan the computer for CA BrightStor registry keys and executables at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Queries the following registry keys for existence:

`HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve Backup\UniversalClientAgent\Common`

`HKLM\SOFTWARE\ComputerAssociates\Cheetah\UniversalClientAgent\Common`

`HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise Backup\UniversalClientAgent\Common`

When the first registry key exists, the plug-in:

- Reads the value of the Path entry
- Returns the following executable pathname:

`FilePathFromRegistry\UnivAgent.exe`

- Creates a SPECIALPGM resource of type DCM

This is the default action as defined in the response file.

2. If the plug-in cannot find any of the registry keys in Step 1, it queries the following registry keys for existence:

`HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve Backup\Base\Path`

`HKLM\SOFTWARE\ComputerAssociates\Cheetah\Base\Path`

HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise Backup\Base\Path

When the first registry key exists, the plug-in:

- Reads the value of the HOME entry
- Returns the following executable pathname:  
`FilePathFromRegistry\carunjob.exe`
- Creates a SPECIALPGM resource of type DCM  
 This is the default action as defined in the response file.

3. If the plug-in also cannot find any of the registry keys in Step 2, it queries the following registry key for existence:

HKLM\SOFTWARE\ComputerAssociates\ARCserveIT\Base\Path

If the registry key exists, the plug-in:

- Reads the value of the HOME entry
- Returns the following executable pathname:  
`FilePathFromRegistry\ASRunJob.exe`
- Creates a SPECIALPGM resource of type DCM  
 This is the default action as defined in the response file.

4. Queries the following registry keys for existence:

HKLM\SOFTWARE\ComputerAssociates\CA\_BAOF\CurrentVersion

HKLM\SOFTWARE\ComputerAssociates\BrightStor Backup Agent for Open Files\CurrentVersion

When the first registry key exists, the plug-in:

- Reads the value of the ServicePath entry
- Creates a SPECIALPGM resource of type DCM for *ServicePathFromRegistry*  
 This is the default action as defined in the response file.

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

### Dr. Watson Plug-In

The coexistence utility runs the Dr. Watson plug-in to scan the computer for Dr. Watson executables at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

- Queries the following pathname for existence:

`%windir%\system32\drwtsn32.exe`

If the file exists, the plug-in creates a SPECIALPGM resource of type DCM.

This is the default action as defined in the response file.

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

### eTrust AV Plug-In

The coexistence utility runs the eTrust AV plug-in to scan the computer for CA Antivirus registry keys and executables at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Reads the following registry key entry values:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\InocIT.Exe\Path

HKLM\SOFTWARE\ComputerAssociates\eTrustITM\CurrentVersion\Path\Home

If one of the entries returns a value, the plug-in creates the following SPECIALPGM resources of type DCM:

- *FilePathFromRegistry\InoRT.exe*
- *FilePathFromRegistry\InoTask.exe*
- *FilePathFromRegistry\InocIT.exe*
- *FilePathFromRegistry\ShellScn.exe*

This is the default action as defined in the response file.

2. Reads the following registry key entry value:

```
HKLM\SOFTWARE\ComputerAssociates\ScanEngine\Path\Engine
```

If the entry returns a value, the plug-in creates the following SPECIALPGM resource of type DCM:

```
FilePathFromRegistry\InoCmd32.exe
```

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

### Scout Plug-In

The coexistence utility runs the Scout plug-in to scan the computer for SurfControl Web Filter for Windows registry keys and executables at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

- Queries the following registry key for existence:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Scscout.Exe
```

If the registry key exists, the plug-in:

- Reads the value of the Path entry
- Returns the following executable pathname:

```
FilePathFromRegistry\scoutsvc.exe
```

- Creates a SPECIALPGM resource of type DCM

This is the default action as defined in the response file.

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

### Windows Plug-In

The coexistence utility runs the Windows plug-in to scan the computer for Windows services and registry keys at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Extracts the directory path of the executable of the service "WinMgmt" (*ServicePath*)
2. Creates the following SPECIALPGM resource of type REGISTRY:

```
ServicePath
```

This is the default action as defined in the response file.

3. Creates the following SPECIALPGM resource of type PBF:

```
%windir%\System32\cidaemon.exe
```

This is the default action as defined in the response file.

#### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

## eTrust Audit Plug-In

The coexistence utility runs the eTrust Audit plug-in to scan the computer for eTrust Audit Version 1.5 registry keys and files before the Privileged Access Manager installation begins, as follows:

1. Queries the following registry key for existence:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\acdistagn.exe
If successful it extracts the "Path" value designated %PathFromRegistry%.
```

If the registry key exists, the plug-in:

- Reads the value of the Path entry
- Returns the following executable pathnames:

```
FilePathFromRegistry\bin\acactmgr.exe
FilePathFromRegistry\bin\SeLogRcd.exe
FilePathFromRegistry\bin\acdistagn.exe
FilePathFromRegistry\acdistsrv.exe
FilePathFromRegistry\acfwrecd.exe
FilePathFromRegistry\acrecorderd.exe
FilePathFromRegistry\aclogrd.exe
FilePathFromRegistry\portmap.exe
FilePathFromRegistry\SeLogRec.exe
FilePathFromRegistry\SeLogRd.exe
FilePathFromRegistry\snmprec.exe
```

This is the default action as defined in the response file. The eTrust Audit plug-in does not add a trusted program (SPECIALPGM) rule by default.

2. Stops the following services:

- "eAudit Action Manager"
- "eAudit Distribution Agent"
- "eAudit Log Router"
- "eAudit Recorder"
- "eAudit Redirector"
- "eAudit Portmap"

If a more recent version of eTrust Audit is installed, it stops the following services:

- "eTrust Audit Action Manager"
- "eTrust Audit Collector"
- "eTrust Audit Distribution Agent"
- "eTrust Audit Distribution Server"
- "eTrust Audit FW-1 Recorder"
- "eTrust Audit Generic Recorder"
- "eTrust Audit Log Router"
- "eTrust Audit Portmap"
- "eTrust Audit Recorder"
- "eTrust Audit Redirector"
- "eTrust Audit SNMP Recorder"

3. When the Privileged Access Manager installation completes, it restarts these same services.

The coexistence utility also runs the eTrust Audit plug-in to:

- Stop the eTrust Audit services when you uninstall Privileged Access Manager
- Start the eTrust Audit services after the Privileged Access Manager uninstall completes

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

**eTrust Audit80 Plug-In**

The coexistence utility runs the eTrust Audit80 plug-in to scan the computer for eTrust Audit r8 registry keys and files at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

- Queries the following registry key for existence:

```
HKLM\SOFTWARE\ComputerAssociates\eTrust Audit\Paths
```

If successful it extracts the "Path" value designated %PathFromRegistry%.

If the registry key exists, the plug-in:

- Reads the value of the RootPath entry
- Creates the following SPECIALPGM resources of type DCM:

```
FilePathFromRegistry\bin\acactmgr.exe
FilePathFromRegistry\bin\SeLogRcd.exe
FilePathFromRegistry\bin\acdistsagn.exe
FilePathFromRegistry\acdistsrv.exe
FilePathFromRegistry\acfwrecd.exe
FilePathFromRegistry\acrecorderd.exe
FilePathFromRegistry\aclogrd.exe
FilePathFromRegistry\portmap.exe
FilePathFromRegistry\SeLogRec.exe
FilePathFromRegistry\SeLogRd.exe
FilePathFromRegistry\snmprec.exe
```

This is the default action as defined in the response file.

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

**F-Secure Antivirus Plug-In**

The coexistence utility runs the F-Secure Antivirus plug-in to scan the computer for F-Secure Anti-Virus registry keys and files, as follows:

- Before the Privileged Access Manager installation begins the plug-in stops the F-Secure Anti-Virus services.
- When the Privileged Access Manager installation completes, the plug-in queries the following registry key for existence:

```
HKLM\SOFTWARE\Data Fellows\F-Secure\Anti-Virus
```

If successful it extracts the "Path" value designated %PathFromRegistry%.

If the registry key exists, the plug-in:

- Reads the value of the Path entry
- Creates the following SPECIALPGM resources of type DCM:

```
FilePathFromRegistry\fssm32.exe
FilePathFromRegistry\fsgk32st.exe
```

This is the default action as defined in the response file. The eTrust Audit plug-in does not add a trusted program (SPECIALPGM) rule by default.

- Whenever the coexistence utility runs, the plug-in:
  - a. Stops the F-Secure Anti-Virus services

- b. Creates the same SPECIALPGM resources it creates when the Privileged Access Manager installation completes (as described earlier in this topic)
- c. Restarts the F-Secure Anti-Virus services

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

**McAfee VirusScan Plug-In**

The coexistence utility runs the McAfee VirusScan plug-in to scan the computer for the McAfee VirusScan service at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Extracts the directory path of the executable of the service "McShield" (*ServicePath*)
2. Creates the following SPECIALPGM resource of type DCM:

```
ServicePath
```

This is the default action as defined in the response file.

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

**Windows Modules Installer Plug-In**

The coexistence utility runs the Windows Modules Installer plug-in to scan the computer for the Windows Modules Install service at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Extracts the directory path of the executable of the service "TrusterInstaller" (*ServicePath*)
2. Creates the following SPECIALPGM resource of type PBF:

```
ServicePath
```

This is the default action as defined in the response file.

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

**Services and Controller Plug-In**

The coexistence utility runs the Services and Controller plug-in to scan the computer for the Windows services management executable at the end of a Privileged Access Manager installation and whenever the utility runs, as follows:

1. Checks if the operating system version is Windows Vista or later  
If the OS is of an earlier Windows version, the plug-in terminates.
2. Creates the following SPECIALPGM resource of type KILL:

```
%windir%\system32\services.exe
```

This is the default action as defined in the response file.

**NOTE**

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

## Resource Hosting Subsystem Plug-In

The Privileged Access Manager installation process runs the Resource Hosting Subsystem plug-in during installation, and the coexistence utility runs the Resource Hosting Subsystem when a customer executes the utility. The Resource Hosting Subsystem plug-in scans the computer for the Cluster Service Element, as follows:

1. Checks if the operating system is Windows Server 2008 or later.  
If the OS is of an earlier Windows version, the plug-in terminates.
2. Checks if the Cluster Service Element is installed on the computer.  
If the Cluster Service Element is not installed, the plug-in terminates.
3. Creates the following SPECIALPGM resource of type PBF:

```
system_drive:\Windows\Cluster\rhs.exe
```

### NOTE

The response file determines the default action that the coexistence utility performs at prescribed stages (what to do before Privileged Access Manager installation, after installation, and so on).

## response.ini Configure the Coexistence Utility

### Valid on Windows

The response file instructs the coexistence utility (eACoexist) what actions to perform when it runs. The response file contains a predefined set of actions for every plug-in that the coexistence utility runs. You can edit the response file to change the default plug-in actions.

### NOTE

The response file pathname is specified in the ResponseFile configuration setting of the SeOSD section. This file is *ACInstallDi\Data\response.ini* by default.

### NOTE

This file has the following format:

```
[Section Name]
Act-Stage-#=Action
...
```

- **Section Name**  
Defines the name of a section that matches a coexistence plug-in.  
The coexistence utility runs the plug-in according to the actions that are defined in this section.
- **Act-Stage-#=Action#**  
Defines the action that you want the plug-in to perform at the prescribed stage.
  - **Stage**  
Specifies the prescribed stage in which you want the plug-in to perform the action, as follows:
    - a. **BeginInstall** The plug-in performs the specified action before Privileged Access Manager starts installing.
    - b. **EndInstall** The plug-in performs the specified action after the Privileged Access Manager installation completes.
    - c. **Utility** The plug-in performs the specified action when you execute the coexistence utility.
    - d. **BeginUninstall** The plug-in performs the specified action before Privileged Access Manager starts the uninstall.
    - e. **EndUninstall** The plug-in performs the specified action after the Privileged Access Manager uninstall completes.
  - **#**  
Specifies the order in which the plug-in executes actions in this stage.
  - **Action**  
Specifies a number that defines the action the plug-in should take, as follows:
    - a. Warn that Privileged Access Manager is not compatible with discovered products.
    - b. Stop services during Privileged Access Manager installation.

- c. Stop services.
- d. Start services.
- e. Create SPECIALPGM rules.
- f. Stop services during Privileged Access Manager uninstall.

### Example: Dr. Watson Plug-in Actions

This example displays the default action the Dr. Watson coexistence plug-in performs by default when discovering the Dr. Watson program on the computer.

```
[DrWatson]
Act-EndInstall-0=5
Act-Utility-0=5
```

This section specifies that when the plug-in runs after a Privileged Access Manager installation completes, it should create SPECIALPGM rules for the program. It also specifies that it should do the same when you execute the utility.

## eACSigUpdate Utility Replace STOP Signature File

### Valid on Windows

The eACSigUpdate utility replaces the local stack overflow protection (STOP) signature file with a file you updated on another computer.

#### NOTE

The eACSigUpdate utility automatically runs when Privileged Access Manager starts, and then at a regular interval, if a signature file broker or a parent Policy Model is defined.

This command has the following format:

```
eACSigUpdate hostname target_file
```

- *hostname*  
Defines the name of the host computer that has the updated the STOP signature file you want to copy to this computer

#### NOTE

For the command to work, you must have administration privileges on the remote host.

- *target\_file*  
Defines the full path and name of the new signature file. This is the location and name of the signature that is retrieved from the specified host.

## eACSyncLockout Utility Synchronize Account Lockout

### Valid on Windows

The eACSyncLockout utility synchronizes an account's lockout with the Privileged Access Manager database. (That is, upon account lockout, the corresponding user's record in the Privileged Access Manager database is suspended.) This utility is effective only when password synchronization is on *and* the user running the utility has the ADMIN property.

This command has the following format:

```
eACSyncLockout -start [-u username] [-p password]
eACSyncLockout -stop|-remove|-debug
```

- *-p password*  
Defines the user password for the service to be installed and started. If -p is not specified, the utility assumes the user has no password.
- **-remove**



Causes the service to be stopped and uninstalled. (In the next boot of the machine, the service does not appear in the Service Control Manager.)

- **-start**  
Causes the service to be installed and started. If -u is not specified, the utility installs and starts the service in the current user's context.
- **-stop**  
Stops the service.
- **-u *user***  
Defines the user context for installing and starting the service.

## issec Utility Display CA Privileged Access Manager Server Control Daemon Status

### Valid on UNIX

The issec utility displays the status of Privileged Access Manager security daemons. If you do not specify any options, the following information appears:

- The Privileged Access Manager version and installation directory
- The status of the Privileged Access Manager kernel extension
- The status of three major daemons: seosd, agent, and watchdog
- The status of daemons: serevu, selogrd, selogrcd, eacws, ReportAgent, policyfetcher, KBLAudMgr
- The status of the PMDB daemon and its name
- The status of the daemons that have been specified in the [daemons] section of seos.ini

This command has the following format:

```
issec [-b] [-k] [-h]
```

- **-b**  
Displays the status and pid of major daemons (seosd, agent, and watchdog).
- **-k**  
Checks if Privileged Access Manager kernel extension is loaded.
- **-h**  
Displays the help for this utility.

## ldap2seos Script Extract Users from LDAP for Adding into CA Privileged Access Manager Server Control

### Valid on UNIX

The ldap2seos utility extracts users from an LDAP database at the server host and adds them to the Privileged Access Manager database.

#### **WARNING**

Privileged Access Manager lets you use LDAP users directly without importing them if the LDAP user store is used by the operating system, that is, it is an enterprise user store. Consider using this functionality of Privileged Access Manager instead of the ldap2seos utility.

The ldap2seos utility extracts information from an LDAP server about the defined users. The extracted information is automatically used to execute selang commands to add the users to the database. The generated commands are also printed to the standard output and saved automatically to the file named /tmp/ldap2seos.tcl.log.

This utility requires access to a TCL shell environment. The ldap2seos script assumes that the TCL shell path is /usr/local/bin/tclsh. If the TCL shell is placed elsewhere, change the first line in the script.

For the utility to work correctly, Privileged Access Manager must be running. The utility updates the database, so a user with the ADMIN privilege must run it. This user must also be authorized in the LDAP database settings to make the search query.

This script has the following format:

```
ldap2seos [options]
```

- **-accfld *account-field***  
Specifies the LDAP field name containing the user ID for Privileged Access Manager.  
If the UNIX user ID is in the LDAP userid field, this option is unnecessary.  
If the UNIX user ID is assigned to an LDAP field other than the userid field, specify the LDAP field as *account-field* and the LDAP userid field is ignored.

#### NOTE

If the script cannot find the userid, users are not uploaded to the Privileged Access Manager database.

- **-b *base-entry***  
Specifies the base entry, in the LDAP database, from which the users are taken. The entry must be valid inside the LDAP database. If the base entry is omitted, LDAP uses the default base entry to provide the users.
- **-d *dn***  
Specifies an entry name to be used with the **-w** switch to authenticate to LDAP as another user; mostly needed to log into LDAP as admin user.
- **-f *filename***  
Specifies a file to which data that are retrieved from the LDAP server can be temporarily stored.
- **-h**  
Displays help for this utility. The screen contains a listing and explanation of ldap2seos usage and options.
- **-h *ldap-host***  
Specifies the name of the host where the LDAP database is located. The default is the local host.
- **-l *ldap-dir***  
Specifies the directory containing the line command utilities that are assumed to be in the bin subdirectory. The default is /usr/local/ldap.
- **-p *port***  
Specifies the port LDAP uses for connections. The default is port 389.
- **-u**  
Identical to **-h**, displays help. The screen contains a listing and explanation of ldap2seos usage and options.
- **-w *bindpasswd***  
Specifies the user password. To be used with the **-d** option where authentication is required to access the LDAP database.

#### Example: Extract User Information

The following command extracts information about users from the LDAP database at host myhost.mysite.com and tries to add them to the Privileged Access Manager database.

```
ldap2seos -h myhost.mysite.com
```

## seos2ldap Script Export CA Privileged Access Manager Server Control Users to LDAP

seos2ldap exports Privileged Access Manager users from the database to an LDAP database at a server host. It extracts appropriate information about users from the Privileged Access Manager database. It then transmits the information to the LDAP database of the selected server. The extracted information is used to generate an LDIF file. Specified users are added to the LDAP database. The responses are saved automatically to the file named /tmp/seos2ldap.tcl.log.

This utility requires access to a TCL shell environment. ldap2seos assumes that the TCL shell path is /usr/local/bin/tclsh. If the TCL shell is placed elsewhere, change the first line in the script.

For the utility to work correctly, Privileged Access Manager must be running. The utility reads from the database, so the user who runs it must have the ADMIN privilege. This user must also be authorized in the LDAP database settings to make changes.

The entry schema, if you elect to use one, for the LDAP database should look like the schema for the Netscape server. If you have changed the Netscape schema, or are using another type of LDAP server, you might need to edit the `seos2ldap` sample script accordingly.

If a Privileged Access Manager database user already appears in the LDAP database, the user is not added. An error message is produced but the export process continues.

This script has the following format:

```
seos2ldap [options]
```

- **-b *base-entry***  
Specifies the base entry, in the LDAP database, that stores user information. The entry must be valid inside the LDAP database. If the base entry is omitted, LDAP prompts the user to provide it.
- **-d *dn***  
Specifies an entry name to be used with the **-w** switch to authenticate to LDAP as another user. This option is required to log into LDAP as an admin user.
- **-f *filename***  
Specifies a file to which data that are retrieved from the LDAP server can be temporarily stored.
- **-h**  
Displays a help for the utility. The screen contains a listing and explanation of `ldap2seos` usage and options.
- **-h *ldap-host***  
Specifies the name of the host where the LDAP database is located. The default is the local host.
- **-l *ldap-dir***  
Specifies the directory containing the line command utilities that are assumed to be in the `bin` subdirectory. The default is `/usr/local/ldap`.
- **-noprompt**  
Cancels base entry prompt. If you did not use the **-b *base-entry*** flag to specify the base LDAP entry, by default `seos2ldap` prompts for a base entry. This flag suppresses the prompt.
- **-p *port***  
Defines the port LDAP uses for connections. The default is port 389.
- **-u**  
Identical to **-h**, displays help. The screen contains a listing and explanation of `ldap2seos` usage and options.
- **-w *bindpasswd***  
Defines the user password. Use this with the **-d** option where authentication is required to access the LDAP database.

### Example: Export User Information

The following command extracts information about users from the Privileged Access Manager database and creates an LDIF file named `SeOS_user_dump`. The command adds records to the LDAP database at host `myhost.mysite.com`. You can edit the LDIF file later and can update LDAP manually.

```
seos2ldap -h myhost.mysite.com
```

## ntimport Utility Import Windows Users and Groups

### Valid on Windows

The `ntimport` utility extracts Windows users and groups from the Windows operating system database for import into a local database. The utility creates the Windows commands necessary to add users and groups to the local Privileged Access Manager database.

**WARNING**

Privileged Access Manager lets use Windows users and groups directly, without needing to import them into the database. Consider using this functionality of Privileged Access Manager instead of the `ntimport` utility, which was developed before Privileged Access Manager could use Windows users and groups directly.

The generated commands are displayed to the standard output. Use the option `-f` if you want to create a file to use as input to the `selang` utility.

This command has the following format:

```
ntimport {-a|{[-u] [-g] [-c]}} [-d] [-U] \
[-D] [-f filename] [-o owner] [-p pmdb] \
[-pa pmdb] [-r remote-host] [-v]
```

- **-a**  
Performs all actions of the `-c`, `-g`, and `-u` switches.
- **-c**  
Generates the `selang` commands that are required to join users to their default groups.
- **-d**  
Imports users and groups with their domain as prefix.
- **-D**  
Retrieves user and group information from the first available domain controller.
- **-f filename**  
Redirects the output to the specified file.
- **-g**  
Generates `selang` commands that are required to import groups from Windows to the local database.
- **-o owner**  
Sets ownership rules for each imported record. Use this flag, to prevent *Administrator* from automatically becoming the owner of all the records. *Owner* is the name of the user or group to be assigned ownership of all records defined by `ntimport`.
- **-p pmdb**  
Generates commands for importing user and groups into the AC environment of the `pmdb`.
- **-pa pmdb**  
Generates commands for importing user and groups into the AC and native environments of the `pmdb`.
- **-pn pmdb**  
Generates commands for importing user and groups into native environment of the `pmdb`.
- **-r remote-host**  
Retrieves user and group information from the specified `remote-host`.
- **-u**  
Generates the `selang` commands that are required to import users from the Windows database to the local database. Names longer than 40 characters are truncated.
- **-U**  
Generates the `selang` commands that are required to import surrogate rules for users.
- **-v**  
Provides the user with progress information. Use this flag to verify the progress of the program when there are many users or groups.

## policydeploy Utility Manage Enterprise Policy Deployment

The `policydeploy` utility manages multiple-rule policies (advanced policy management). The utility stores policy versions on DMS nodes, assigns policies to hosts and host groups, and unassigns these policies. You can also directly deploy or undeploy a stored policy or upgrade deployed policies to the latest version.

The utility handles several tasks and has the following functions:

Task	Function
Assign or unassign a policy	<code>policydeploy -assign</code>
Delete a policy	<code>policydeploy -delete</code>
Deploy a policy	<code>policydeploy -deploy</code>
Undeploy a policy	<code>policydeploy -undeploy</code>
Re-execute a deployment task	<code>policydeploy -fix</code>
View deployment scripts	<code>policydeploy -getrules</code>
Join or remove a host to a host group	<code>policydeploy -join</code>
Migrate a PMD to advanced policy management	<code>policydeploy -migrate</code>
Reset policy deployment	<code>policydeploy -reset</code>
Restore all policies	<code>policydeploy -restore</code>
Store a policy	<code>policydeploy -store</code>
Upgrade a policy version	<code>policydeploy -upgrade</code>
Downgrade a policy version	<code>policydeploy -downgrade</code>

## policydeploy -assign Function Assign or Unassign a Policy

This function assigns or unassigns the specified policy to one or more hosts or host groups.

This function has the following format:

```
policydeploy -assign[-] name -hnode|-ghnode list [-dms list]
```

- **-assign *name***  
Assigns the specified policy to one or more hosts or host groups.
- **-assign- *name***  
Unassigns the specified policy from one or more hosts or host groups.
- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+(new_dms_name)
```

### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-ghnode *list***  
Defines a comma-separated list of host groups (GHNODE objects) that you want to assign the policy to.
- **-hnode *list***

Defines a comma-separated list of hosts (HNODE objects) that you want to assign the policy to.

### Example: Assign an IIS 5 Protection Policy

The following example shows you how to assign a policy for securing Internet Information Services (IIS) 5 web servers. We will review the policy and the latest (fourth) version of policy IIS5 and then assign the policy to a host group called IIS5Servers. Policy IIS5 is stored on the crDMS@cr\_host.company.com DMS node.

1. Connect to the DMS using selang:

```
hosts crDMS@cr_host.company.com
```

You can now query our DMS via selang.

2. If you're not sure what is the latest finalized version of the policy, issue the following selang command to find all versions of the policy:

```
sr GPOLICY IIS5
```

The selang window lists the properties of the IIS5 policy, including the Final Policy, which is the latest version of the policy that you can assign (finalized).

3. Issue the following selang command to view the policy deployment and undeployment scripts:

```
sr RULESET IIS5#04
```

The selang window displays the IIS5#04 RULESET object, including the deployment and undeployment rules that relate to the fourth version of the IIS5 policy.

4. In a command prompt window, run the policydeploy utility:

```
policydeploy -assign IIS5 -ghnode IIS5Servers
```

This assigns the IIS5 policy to all hosts in the IIS5Servers logical host group, and in turn deploys the fourth version of the IIS5 policy on these hosts.

### Example: Unassign an IIS 5 Protection Policy

The following example shows you how to unassign an assigned IIS 5 policy from the web servers that we assigned it to in the previous example.

In a command prompt window, run the policydeploy utility:

```
policydeploy -assign- IIS5 -ghnode IIS5Servers
```

This unassigns the IIS5 policy from all hosts in the IIS5Servers logical host group, and in turn undeploys the version of the IIS5 policy that is deployed on these hosts.

### policydeploy -delete Function Delete a Policy

This function deletes the specified policy or policy version.

#### NOTE

Before you delete a policy, remove any policy dependencies. Before you delete a policy or policy version, undeploy or unassign the policy or policy version from all hosts and host groups.

You cannot delete a policy or policy version if:

- It is a prerequisite for another policy.
- It is assigned to a host or host group.
- It is deployed on a host or host group.
- It has a status of Undeployed with failures.
- It has a status on the DMS.

This function has the following format:

```
policydeploy -delete name[#xx] [-dms list]
```

- **-delete *name* [#xx]**  
Deletes the specified policy or policy version.
- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+ (new_dms_name)
```

#### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

### Example: Delete an Unassigned IIS 5 Protection Policy

The following example shows you how to delete an unassigned IIS 5 policy from the DMS. In this example, policy IIS5 is not assigned to any hosts or host groups and is stored on the `crDMS@cr_host.company.com` DMS node.

To delete the IIS 5 protection policy, open a command prompt window and run the `policydeploy` utility:

```
policydeploy -delete IIS5
```

Policy IIS5 is deleted from the `crDMS@cr_host.company.com` DMS node.

### Example: Delete an IIS 5 Protection Policy Version

The following example shows you how to delete the unassigned policy version IIS5#05 from the DMS. In this example, policy version IIS5#05 is not assigned to any hosts or host groups and is stored on the `crDMS@cr_host.company.com` DMS node.

To delete the IIS 5 protection policy version, open a command prompt window and run the `policydeploy` utility:

```
policydeploy -delete IIS5#05
```

Policy version IIS5#05 is deleted from the `crDMS@cr_host.company.com` DMS node.

## policydeploy -deploy Function Deploy or Undeploy a Policy

This function deploys and undeploys policies on the specified endpoints, without assigning policies to a host or unassigning policies from a host.

This function has the following format:

```
policydeploy { -deploy name[#xx] | -undeploy name[#xx] } {-nodelist hnode_list | -root dbs} [-dms list]
```

- **-deploy *name* [#xx]**  
Prompts you for whether you want to directly deploy the specified stored policy version (without assigning the policy to the host) on defined endpoints. To deploy the latest stored version of the policy, omit the policy version number.
- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.

If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+(new_dms_name)
```

#### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-nodelist *hnode\_list***  
Defines a comma-separated list of hosts (HNODE objects) that you want to perform the operation for.
- **-root *dbs***  
Defines a comma-separated list of databases where the policy should be deployed or undeployed.

#### NOTE

If the root database is a Policy Model parent, the policy is deployed or undeployed throughout its subscribing databases. If the root database is a Privileged Access Manager endpoint, the policy is deployed or undeployed on the specified database only. This option is for backward compatibility with r8 SP1 databases and PMDBs.

- **-undeploy *name*[#*xx*]**  
Prompts you for whether you want to directly undeploy the specified policy version *name*#*xx* (without unassigning the policy) from defined endpoints.  
To undeploy the latest stored version of the policy, omit the policy version number.

## policydeploy -fix Function Re-execute Deployment Task

This function fixes the specified deployment task or package and redeploys the task or package.

This function has the following format:

```
policydeploy -fix {-task list | -package list} [-dms list]
```

- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+(new_dms_name)
```

#### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-fix**

#### NOTE

Fixes and redeploys the specified deployment task or package.

- **-package *list***  
Defines a comma-separated list of deployment packages (GDEPLOYMENT).
- **-task *list***



Defines a comma-separated list of deployment tasks.

## policydeploy -getrules Function View Deployment Scripts

This function lets you view the selang deployment and undeployment scripts for the specified policy version.

```
policydeploy -getrules name[#xx] -ds file1 -uds file2 [-dms list]
```

- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following selang command after you create a new DMS using dmsmgr:

```
so dms+(new_dms_name)
```

### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-ds *file1***  
Specifies the path name of the file containing the deployment rules. These are the commands necessary to construct the policy. When you use the -getrules option, the utility creates this file.

### WARNING

Policy deployment does not support commands that set user passwords. Do not include such commands in your deployment script file. Native selang commands are supported but do not appear in deviation reports.

- **-getrules *name[#xx]***  
Retrieves the selang deployment and undeployment scripts for the specified policy version. If you do not specify a policy version, the command applies to the latest policy version.
- **-uds *file2***  
Defines the path name of the file containing the rules required to undeploy the policy. These are the commands necessary to undeploy the policy. When you use the -getrules option, the utility creates this file.  
When Privileged Access Manager undeploys a policy, if there is no policy undeployment script stored, Privileged Access Manager calculates the commands required to remove the policy.

## Example: View the Deployment Scripts Associated with an IIS 5 Protection Policy

The following example shows you how to view the selang scripts associated with deploying and undeploying a policy for securing Internet Information Services (IIS) 5 web servers. The name of the policy is myPolicy.

To view the selang scripts, run the following command:

```
policydeploy -getrules myPolicy -ds c:\folder\deployRules.txt -uds undeployRules.txt
```

## policydeploy -join Function Join or Remove a Host to a Host Group

This function joins a host to a host group or removes a host from a host group.

This function has the following format:

```
policydeploy -join[-] hnode_name -ghnode name [-dms list]
```

- **-dms *list***

(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.

If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+(new_dms_name)
```

#### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- `-ghnode name`  
Defines the name of the host group for the operation you want to perform.
- `-join hnode_name`

#### NOTE

Adds the specified host to the host group.

- `-join- hnode_name`

#### NOTE

Removes the specified host from the host group.

## policydeploy -migrate Function Migrate a PMD to Advanced Policy Management

This function migrates a PMD to the advanced policy management environment. When you migrate a PMD to advanced policy management, you create policies from the rules in the PMD, create a host group and hosts in the DMS, and assign the policies to the host group.

This function has the following format:

```
policydeploy -migrate pmdName@hostName [-dms name] [-policydir directory] \
[-exportfilter "class, class..."] [-hgcreate] [-pcreate name] [-addpmdfilter]\
[-unsubs] [-delete] [-auto]
```

- `pmdName@hostName`  
Defines the name of the PMD to migrate.
- `-dms name`  
(Optional) Defines the name of the DMS that the rules in the PMD will be migrated to. If you do not specify the DMS name, the DMS name is retrieved from the Privileged Access Manager database on the local host.

#### NOTE

If you do not specify a DMS name and there is more than one DMS name specified in the Privileged Access Manager database on the local host, the rules in the PMD are migrated to all specified DMSs.

- `-policydir directory`  
(Optional) Defines the directory in which the policy file is stored. If you do not specify a directory, the policy file is stored in your current working directory.  
The name of the policy file is `pmdName_hostName_policy`.
- `-exportfilter "class, class..."`  
(Optional) Specifies the Privileged Access Manager classes to export from the PMD database. If you do not specify any classes, all classes in the PMD database are exported.  
The following points apply to the `-exportfilter` parameter:

If you export rules that modify resources in a particular class, and the class has a corresponding resource group, Privileged Access Manager also exports the rules that modify resources in that resource group.

If you export rules that modify resources in a particular resource group, Privileged Access Manager also exports the rules that modify the member resource of the resource group.

If you export rules that modify resources in a particular class and that class has a PACL, Privileged Access Manager also exports the rules that modify resources in the PROGRAM class.

If you export rules that modify resources in a particular class and that class has a CALACL, Privileged Access Manager also exports the rules that modify resources in the CALENDAR class.

If you export rules that modify resources in a particular class, and one of the resources in that class is a member of a CONTAINER resource group, Privileged Access Manager exports the rules that modify resources in the CONTAINER class and the rules that modify the resources that are members of each CONTAINER resource group.

- **-hgcreate**  
(Optional) Creates a host group (GHNODE object) on the DMS that corresponds to *pmdName*, creates hosts (HNODE objects) on the DMS that correspond to endpoint subscribers of *pmdName*, and joins the hosts to the host group.
- **-pcreate *name***  
(Optional) Creates a POLICY object on the DMS that contains the rules in the policy file that was exported from *pmdName*, and assigns the POLICY object to the host group on the DMS that corresponds to *pmdName*. If you specify *name*, the created POLICY object is named *name\_POLICY#01*; if you do not specify *name*, the created POLICY object is named *pmdName\_POLICY#01*.
- **-addpmdfilter**  
(Optional) Applies a filter file to *pmdName*. The filter file is named filter.flt and is located in the same directory as *pmdName*.

#### NOTE

You use the filter file to create a password PMD. The filter file lets only user password commands be sent to the subscribers of *pmdName*.

- **-unsubs**  
(Optional) Unsubscribes endpoint subscribers from *pmdName*.
- **-delete**  
(Optional) Deletes *pmdName* after the policydeploy -migrate function has finished executing.
- **-auto**  
(Optional) Specifies to execute both the -hgcreate and -pcreate options. This option does the following:
  - Exports the rules in *pmdName*
  - Creates a host group (GHNODE object) on the DMS that corresponds to *pmdName*
  - Creates hosts (HNODE objects) on the DMS that correspond to endpoint subscribers of *pmdName*
  - Joins the hosts to the host group
  - Creates a POLICY object on the DMS that contains the rules in the policy file that was exported from *pmdName*
  - Assigns the POLICY object to the host group on the DMS that corresponds to *pmdName*

#### Example: Migrate Rules and Create a Host Group

This example migrates the rules from Master PMD on host A to DMS\_\_ on host B, saves the policy file to the C:\Data\policies\_MasterPMD\_hostA directory, creates a host group named MasterPMD on DMS\_\_, creates hosts on DMS\_\_ that correspond to the endpoint subscribers of Master PMD, and joins the hosts to the MasterPMD host group:

```
policydeploy -migrate MasterPMD@hostA -dms DMS__@hostB -policydir "C:\Data\policies_MasterPMD_hostA" -hgcreate
```

## policydeploy -reset Function Reset Policy Deployment

This function resets policy deployment on the endpoint. Privileged Access Manager undeploys all the effective policies on the endpoint, deletes all advanced policy management properties, and resets host status.

This function has the following format:

```
policydeploy -reset hnode_name [-dms list]
```

- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following selang command after you create a new DMS using dmsmgr:

```
so dms+(new_dms_name)
```

### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-reset *hnode\_name***  
Resets policy deployment on the specified endpoint.

## policydeploy -restore Function Restore All Policies

This function undeploys any policies on the specified host, then restores (directly redeploys) all the policies that should be deployed (assigned or directly deployed) on the host by resending all the deployment tasks to the host for execution.

This function has the following format:

```
policydeploy -restore hnode_name [-dms list]
```

- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following selang command after you create a new DMS using dmsmgr:

```
so dms+(new_dms_name)
```

### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-restore *hnode\_name***

### NOTE

Restores (directly redeploys) all the policies that should be deployed on the specified host.

## policydeploy -store Function Store a Policy

This function stores the specified policy on the DMS nodes specified by the command or in the local Privileged Access Manager database. Unless you use the `-silent` option, you need to confirm this action at the prompt.

If no previous version of the specified policy is stored on the DMS, version 1 of the policy is created (*name#01*). If a previous version of this policy exists, a new version of the policy is created (*name#last\_version+1*). The policy version you store is automatically finalized. When you need to update a policy, you must store a new version of the policy that contains the required modified policy deployment and undeployment rules.

This function has the following format:

```
policydeploy -store name -ds file1 [-uds file2] [-dms list] [-desc description] [-prereq list] [-silent]
```

- **-desc *description***  
(Optional) Defines the business description for the policy.
- **-dms *list***  
(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.  
If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following `selang` command after you create a new DMS using `dmsmgr`:

```
so dms+(new_dms_name)
```

### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-ds *file1***  
Specifies the path name of the file containing the deployment rules. These are the commands necessary to construct the policy. When you use the `-getrules` option, the utility creates this file.

### WARNING

Policy deployment does not support commands that set user passwords. Do not include such commands in your deployment script file. Native `selang` commands are supported but do not appear in deviation reports.

- **-prereq *list***  
(Optional) Defines a comma-separated list of policies that must be deployed before you can deploy this policy.

### WARNING

If a prerequisite policy is not deployed when you try to deploy a dependent policy, the deployment task's status is changed to *Pending Prerequisite* and the deployment resumes when all prerequisite policies are deployed. Similarly, if you try to undeploy a policy that is a prerequisite to another deployed policy, the deployment task's status is changed to *Pending Dependents* and the deployment resumes when all dependent policies are undeployed.

- **-silent**  
(Optional) Suppress the confirmation prompt for the requested action.
- **-store *name***  
Stores the specified policy on the specified DMS nodes or in the local Privileged Access Manager database.  
**Note:** Policy names cannot include the `#` (hash) character which is reserved for denoting policy version numbers and is added automatically.
- **-uds *file2***  
Defines the path name of the file containing the rules required to undeploy the policy. These are the commands necessary to undeploy the policy. When you use the `-getrules` option, the utility creates this file.

When Privileged Access Manager undeploys a policy, if there is no policy undeployment script stored, Privileged Access Manager calculates the commands required to remove the policy.

### Example: Store an IIS 5 Protection Policy

The following example shows you how to store a policy for securing Internet Information Services (IIS) 5 web servers. This is the first time we store this policy on the DMS.

#### NOTE

The selang commands in this example are for resources on a Windows operating system but the same procedure also applies on UNIX.

1. Save a file named IIS5.selang with the following IIS script:

```
# IIS5 deployment script
eu inet_pers owner(nobody)
er FILE c:\InetPub\wwwroot\* defaccess(none) owner(nobody)
authorize FILE c:\InetPub\wwwroot\* uid(inet_pers) access(all)
er FILE c:\InetPub\wwwroot\scripts defaccess(none) owner(nobody)
er FILE *.asp defaccess(none) owner(nobody)
authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read, execute)
```

These are the commands necessary to deploy an IIS 5 protection policy.

2. Save a file named IIS5\_rm.selang with the following script:

```
# IIS5 undeployment script
ru inet_pers
rr FILE c:\InetPub\wwwroot\*
rr FILE c:\InetPub\wwwroot\scripts
rr FILE *.asp
```

These are the commands necessary to undeploy the IIS 5 protection policy we created in Step 1.

3. Open a command prompt window and run the policydeploy utility:

```
policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang -desc "IIS5 web server security policy" -
silent
```

This stores on the DMS the policy IIS5 (GPOLICY object) and the first version of the policy (IIS5#01 POLICY object) with the scripts defined in IIS5.selang and IIS5\_rm.selang.

## policydeploy -upgrade Function Upgrade or Downgrade a Policy Version

This function upgrades a policy to its latest finalized version on the defined hosts, or downgrades a policy to a specified policy version on the defined hosts.

This function has the following format:

```
policydeploy {-upgrade name | -downgrade name#xx} [-nodelist hnode_list|-ghnode name] [-list] [-dms name]
```

- **-dms list**

(Optional) Specifies a comma-separated list of DMS nodes to use. When you deploy or undeploy a policy, these are the DMS nodes to which the action is reported. When you store a policy, these are the DMS nodes where the policy is stored.

If you do not specify DMS nodes with this option, the utility uses the list of DMS nodes specified in the local Privileged Access Manager database. To specify a list of DMS nodes in the database, you need to issue the following selang command after you create a new DMS using dmsmgr:

```
so dms+(new_dms_name)
```

#### NOTE

You need to issue the same command if you did not specify the DMS node during installation, or if you want to replace or add the registered DMS on the endpoint. However, when you specify to create an advanced

policy management server during installation, the DMS is added to the database and you do not need to manually run the above command.

- **-downgrade *name#xx***  
Downgrades a policy to the specified policy version on the defined hosts.
- **-ghnode *name***  
Defines the name of the host group for the operation you want to perform.
- **-list**  
(Optional) Lists the hosts that have a version of the specified policy deployed, that is not the version specified. If you use **-upgrade** the implicitly specified version is the latest available.
- **-odelist *hnode\_list***  
Defines a comma-separated list of hosts (HNODE objects) that you want to perform the operation for.
- **-upgrade *name***  
Upgrades the specified policy to its latest finalized version on the defined hosts.

### Example: Upgrade an IIS 5 Protection Policy

The following example shows you how to upgrade a policy. We will first review the deployment to see which hosts do not have the latest version of this policy deployed.

1. In a command prompt window, run the policydeploy utility:

```
policydeploy -upgrade IIS5 -list
```

This lists the hosts that have an older version of the IIS5 policy deployed.

2. Upgrade all of these hosts to the latest version of the policy:

```
policydeploy -upgrade IIS5
```

### Example: Downgrade an IIS 5 Protection Policy

The following example shows you how to downgrade a policy. We will first review the deployment to see which hosts have a deployed policy that has earlier versions.

1. In a command prompt window, run the policydeploy utility:

```
policydeploy -downgrade IIS5#3 -list
```

This lists the hosts that have a version of the IIS5 policy deployed that is later than version 3.

2. Downgrade all of these hosts to the third version of the policy:

```
policydeploy -downgrade IIS5#3
```

## ReportAgent Utility Send Report Snapshots and Audit Events

The ReportAgent sends report snapshots and audit events to the Distribution Server for inclusion in Privileged Access Manager, UNIX Authentication Broker, and Audit Log reports.

Configure an endpoint for reporting before you run the ReportAgent. When you configure an endpoint for reporting, you specify the Distribution Server with which the ReportAgent communicates and the schedule at which it runs. After you configure an endpoint for reporting, the ReportAgent runs as a daemon or service and sends snapshots at the scheduled times. However, to send report snapshots or audit events to the Distribution Server immediately, run the ReportAgent on demand.

**Note:** For more information about how to configure an endpoint for reporting, see the *Implementation Guide*. You can also use the `report_agent.sh` script to configure, start, and stop the ReportAgent on UNIX computers.

On UNIX computers, you run the ReportAgent utility from the `ACSharedDir/bin` directory, where `ACSharedDir` is the default directory `/opt/CA/PAMSCShared`. You may also need to set the library path environment variable.

This command has the following syntax:

```
ReportAgent -debug {0 | 1 | 2} -task {0 | 1 | 2 | 3 | 4} [-now]
```

```
ReportAgent -report snapshot
```

- **-debug {0 | 1 | 2}**  
Specifies to run the ReportAgent in debug mode. The ReportAgent service or daemon must be stopped to use this option.  
**Limits:** 0Prints debug information to the console.  
1Prints debug information to the log file.  
2Does not print debug information (no output).
- **-task {0 | 1 | 2 | 3 | 4}**  
Specifies the information that the ReportAgent sends to the Distribution Server.  
**Limits:** 0Sends a snapshot of the Privileged Access Manager database and any local PMDBs to the queue/snapshots queue on the Distribution Server.  
1Sends endpoint audit events to the queue/audit queue on the Distribution Server.  
2(UNIX) Sends a snapshot of the UNIX Authentication Broker database to the ac\_endpoint\_to\_server queue on the Distribution Server.  
3(UNIX) Sends UNIX Authentication Broker audit events to the queue/audit queue on the Distribution Server.  
4(UNIX) Sends keyboard logger audit events to the queue/audit queue on the Distribution Server.
- **-now**  
Run the ReportAgent immediately.  
If you do not specify this option, the ReportAgent runs at the next scheduled time.
- **-report snapshot**  
Send a snapshot of the Privileged Access Manager database and any local PMDBs to the queue/snapshots queue on the Distribution Server immediately. The ReportAgent service or daemon must be running to use this option.

#### Example: View ReportAgent Debug Information

The following example sets the library path environment variable on a Linux computer, then specifies the following actions:

- To run the ReportAgent in debug mode immediately
- To print debug information to the console
- To send audit events to the Distribution Server

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/PAMSCShared/lib
```

```
export LD_LIBRARY_PATH
```

```
cd /opt/CA/PAMSCShared/bin
```

```
./ReportAgent -debug 0 -task 1 -now
```



## ReportAgent Log Files

The following table lists the log files to which the ReportAgent writes debug information when you run the ReportAgent -debug 1 command. In this table, *ACSharedDir* is the default directory /opt/CA/PAMSCShared and *ACInstallDir* is the directory in which you installed Privileged Access Manager:

ReportAgent Option	UNIX Log File	Windows Log File
-task 0	<i>ACSharedDir</i> /log/ac2xml.log	<i>ACInstallDir</i> \log\ac2xml.log
-task 1	<i>ACSharedDir</i> /log/ac2elm.log	<i>ACInstallDir</i> \log\ac2elm.log
-task 2	<i>ACSharedDir</i> /log/unab2xml.log	-
-task 3	<i>ACSharedDir</i> /log/unab2elm.log	-
-task 4	<i>ACSharedDir</i> /log/kbl2elm.log	-

## report\_agent.sh Script Configure the Report Agent

### Valid on UNIX

The report\_agent.sh script lets you configure the Report Agent daemon after installation. Use the report\_agent.sh script if you need to change the Report Agent configuration settings you set when you installed Privileged Access Manager.

The report\_agent.sh script is located in *ACSharedDir*/lbin. By default, this directory is /opt/CA/PAMSCShared/lbin.

This command has the following format:

```
report_agent.sh start
```

```
report_agent.sh stop
```

```
report_agent.sh config -server##hostname [-proto {ssl|tcp}] [-port port_number] [-rqueue queue_name] \
```

```
[-schedule <time@day[,day2,...]>] [-audit] [-bak] [-silent]
```

- **config**  
Specifies that the remaining parameters configure the Report Agent daemon.
- **start**  
Starts the Report Agent.
- **stop**  
Stops the Report Agent.
- **-server *hostname***  
Defines the name of the Distribution Server host. Combined with the input from the -port option, the script constructs the Distribution Server URL and sets the report\_server configuration setting in the ReportAgent section.
- **-audit**  
Specifies whether you want to send endpoint audit data to the Distribution Server. This sets the reportagent\_enabled configuration setting in the ReportAgent section.
- **-bak**  
Specifies to keep timestamped backups of audit files. This sets the logmgr section configuration setting Backup\_Date to yes and audit\_max\_files to 50.
- **-port *port\_number***

Defines the port number to use for communication with the Distribution Server. Combined with the input from the `-server` option, the script constructs the Distribution Server URL and sets the `report_server` configuration setting in the ReportAgent section.

- **-proto**  
Specifies the connection protocol (TCP or SSL). This sets the `use_ssl` configuration setting in the ReportAgent section
- **-rqueue *queue\_name***  
Defines the name of the queue to which the Report Agent sends snapshots of the local database and any PMDBs. This sets the `send_queue` configuration setting in the ReportAgent section.
- **-schedule *<time@day[,day2,...]>***  
Defines when to generate reports and when to send the reports to the Distribution Server.
- **-silent**  
Specifies not to ask for confirmation.

### Example: Configure the Report Agent

This example sets the Report Agent to send database snapshots to a Distribution Server on `rscomp.com` using port 61616 over SSL and a queue named `queue/snapshots`. It also enables sending audit data to the Distribution Server and sets backup settings for the audit log file:

```
report_agent.sh config -server rscomp.com -proto ssl -port 61616 -rqueue queue/
snapshots -audit
```

Once you configure Report Agent, you should update the `+reportagent` user with a correct password (shared secret) that the Distribution Server expects. To do this, enter the following:

```
eu +reportagent epassword(Shared_Secret) nonnative
```

## seaudit Utility Display Audit Log Records

The `seaudit` utility displays the records in the Privileged Access Manager audit log file. To execute the `seaudit` utility on Windows, you must have the `AUDITOR` attribute and must belong to the `audir_group` in `seos.ini`. When displaying audit records that include passwords, `seaudit` protects the password identity by substituting a series of asterisks (`***`) in place of the password text.

### NOTE

You can use the string matching in the command switches and options. Some UNIX shells automatically expand mask arguments; therefore, when invoking `seaudit` from such a shell, prevent the masks from being handled by the shell by typing a backslash (`\`) before an asterisk or question mark.

### NOTE

The `seaudit` utility displays trace records by user name, not by user ID.

This command has the following format:

```
seaudit switch [options]
```

- **switch**  
Defines the mode of operation for the utility. Can be *one* of the following options:
  - **-a | -all**  
Displays all records except the user trace records sent to the audit log by the tracing facility.

**NOTE**

The connected TCP records, which are available for UNIX, are also not displayed. Specify the `-c` option to display these records.

- **-, | -help**  
Displays the help for this utility.
- **{-i | -inet} *host service***  
Displays the INET audit records of the TCP requests received from the specified hosts for the specified services. Both *host* and *service* are masks that identify the set of hosts and services that seaudit searches for. On UNIX, to list the TCP records with the network ID (port number) to which connection was made, add the `-c` flag. For example:  
  

```
seaudit -i -c myhost telnet
```
- **{-l | -login} *user1, user2, ... terminal***  
Displays the LOGIN records for the comma-separated specified users, on the specified terminal. Both *user* and *terminal* are masks. On UNIX, this also lists records that are created by serevu when it enables and disables users, and records that are created by the authorization daemon when an invalid password is entered.
- **{-r | -resource} *class resource user1, user2, ...***  
Displays the general resources audit of the specified class on the specified resource for the specified comma-separated users.
  - a. *class* is a mask that identifies the class to which the accessed resource belongs.
  - b. *resource* is a mask that identifies the names of the resources that were accessed.
  - c. *user* is a mask of the name of the user who accessed the resource.
- **-s | -start**  
Displays the Privileged Access Manager startup and shutdown messages.
- **-St | -Stat *message\_number***  
(UNIX only). Displays a description of the watchdog message number.
- **-t | -table**  
Displays the table of log codes.
- **-tr**  
Displays trace records of all the users whose activities are being traced.  
**Note:** Trace records display the login session ID column by default. If you do not want to display this column, use the `-format` option.
- **-trr *resource***  
Displays the trace records of the specified resource.
- **-tru {*uid1|user1*}, {*uid1|user2*}, ...**  
Displays the trace records of the users with the specified numeric uids or user names.
- **-u *command class record user***  
Displays database update audit records:
  - a. *command* is a mask identifying the set of selang commands to search for.
  - b. *class* is a mask identifying the classes to search for.
  - c. *record* is a mask identifying the records to search for.
  - d. *user* is a mask identifying the users who executed the commands.
- **-w**  
Displays the watchdog audit records.

**NOTE**

The user trace does not record an event when a user deletes an internally protected file.

- **options**

Defines optional modifiers that change the way that the utility displays its information. Can be one or more of the following options:

- **-c**

(UNIX only). Displays the *connected* INET records. These records are generated for session ID tracking, which list the port number of successful TCP connections.

For example, a user (user1) opens a Telnet session from comp1 to comp2, both with Privileged Access Manager installed. Privileged Access Manager on comp2 can be configured (logconnected configuration setting) to send the acknowledgement to comp1 with the credentials of the user who logged in through the Telnet session (this may be a user other than user1). When comp1 receives this acknowledgement, it creates a TCP-CONNECTED record (a session establishment record) that can then be displayed using the -c option.

- **-detail**

Displays detailed information about each record.

- **-delim *delimiter***

Defines the delimiter to use before the first field and between the remaining fields. For example, the following command makes fields appear in quotation marks that are separated by a comma:

```
seaudit -a -delim \,
```

- **-delim2 *delimiter***

Same as the -delim option, except that the delimiter does not appear before the first field.

- **-delim3 *delimiter***

Same as the -delim option, except that it includes a delimiter between day, month, and year.

- **-delim4 *delimiter***

Same as the -delim2 option.

- **-ed *date***

Specifies the end date. Records that are logged after this date are *not* displayed.

You can specify the *date* in one of two ways:

- Using the format *dd-mm-yyyy*.
- Using the string *today* to set the date as today.

You can also use the string *today* followed by - (minus) and a number. This defines the date as the specified number of days before today. For example, *today-3* means that the date is three days ago.

- **-et *time***

Specifies the end time. Records that are logged after this time are *not* displayed.

You can specify *time* in one of two ways:

- Using the 24-hour format *hh:mm*
- Using the string *now* to set the time as now.

You can also use the string *now* followed by - (minus) and a number. This defines the time as the specified number of minutes before now. For example, *now-60* means that the time is sixty minutes (one hour) ago. To delineate a time frame within a particular day, use this option with -sd, -ed or both.

**Note:** The *now* string is valid for the present day's time. For example, if the present time is 130 am, you specify *now-89*. If you specify *now-90*, then no records appear.

- **-f | -failure**

Specifies *not* to display access failures.

- **{-fn | -file} *fileName***

Specifies the name of the audit log file to be searched.

- **-format *release***

Specifies that the output format looks like it did for the Privileged Access Manager *release*.

*release* Defines the release number. The valid values are:

- a. **80sp1** The output in r8 SP1 did not include the effective UID column that exists in newer releases.
- b. **12** The output in r12.0 did not include the ability to display password change records. For trace records, the output in r12.0 also did not include the login session ID information.

- **-g | -grant**  
Specifies *not* to display successful (granted) accesses.
- **-gn | -grantnotify**  
Specifies *not* to display successful (granted) accesses, except for notify records.
- **-kbl -a -sid *sid* {-rp | -pr | -cmd | -exe | -disp}**  
(UNIX only) Specifies to display the content of the keyboard logging audit file (kbl.audit).
  - **-a**  
Displays all recorded sessions in the audit file.
  - **-sid *sid***  
Specifies the keyboard logging session ID.
  - **-rp**  
Replays the entire keyboard logging session.
  - **-pr**  
Displays the entire keyboard logging session, excluding control characters.
  - **-cmd**  
(UNIX Only) Displays the commands that the user entered during the command line logging session.
  - **-exe**  
Displays the EXECARGS details of commands that the user executed in the shell.
  - **-disp**  
Specifies to display the recorded session time.

#### NOTE

You can run the command in the following shells: bash, tcsh, csh, ksh, jsh, rsh, ash, zsh

- **-logout**  
(UNIX only) Specifies *not* to display logout records.
- **-millennium**  
(UNIX only) Specifies that years be displayed with four digits instead of two.
- **-n | -netaddr**  
Specifies that the internet addresses should be displayed instead of host names in TCP/IP records.
- **-notify**  
Specifies *not* to display NOTIFY audit records.
- **{-o | -origin} *host***  
Specifies that only records originating from the specified host be displayed.  
This option is only applicable when browsing records from a consolidated audit file that is created by the selogrcd log-routing collection daemon.
- **-pwa**  
(UNIX only) Specifies *not* to display password attempt records.
- **-sd *date***  
Specifies the start date. Records that logged prior to this date are *not* displayed.  
You can specify the *date* in one of two ways:
  - Using the format *dd-mm-yyyy*.
  - Using the string *today* to set the date as today.
 You can also use the string *today* followed by - (minus) and a number. This defines the date as the specified number of days before today. For example, *today-3* means that the date is three days ago.
- **sessionid**  
Specifies to show a column that contains user login session ID information. This column is hidden by default.

**NOTE**

This option is valid only for endpoints with r12.0 SP1 and above.

- **-st *time***

Specifies the start time. Records that logged before this time are *not* displayed.

You can specify *time* in one of two ways:

- Using the 24-hour format *hh:mm*
- Using the string *now* to set the time as now.

You can also use the string *now* followed by - (minus) and a number. This defines the time as the specified number of minutes before now. For example, *now-60* means that the time is sixty minutes (one hour) ago. To delineate a time frame within a particular day, use this option with *-sd*, *-ed* or both.

**Note:** The *now* string is valid for the present day's time. For example, if the present time is 130 am, you specify *now-89*. If you specify *now-90*, then no records appear.

- **-v | -servnum**

Specifies that port numbers are displayed instead of service names.

- **-warn**

Specifies *not* to display warning records.

**Examples**

- To list all audit records since 3 January 2004, use the following command:

```
seaudit -a -sd 04-Jan-2004
```

- To list the failed logins of the user root from any terminal on 3 January 2004, use the following command:

```
seaudit -sd 04-Jan-2004 -ed 04-Jan-2004 -l root * -g
```

- To list all accesses of user John to every resource of class FILE, use the following *command*:

```
seaudit -r FILE "*" John
```

- To list all audit records that were logged between 17:00 (the first day) and 08:00 (the following day), for all dates, use the following command:

```
seaudit -a -st 17:00 -et 08:00
```

- To list all audit records that were logged between 08:00 and 17:00, use the following command:

```
seaudit -a -st 08:00 -et 17:00
```

- To list all warning records for logins and resource accesses for a single user, use the following command:

```
seaudit -login * * -resource * * * -grant -failure -logout -pwa
```

- To list all login records for two users, use the following command:

```
seaudit -login "user1, user2"
```

- To list all audit records from yesterday, use the following command:

```
seaudit -a -sd today-1 -ed today-1
```

- To list all the audit records in the kbl.audit log file, use the following command:

```
seaudit -kbl
```

- To display all the recorded sessions in the audit file, use the following command:

```
seaudit -kbl -a
```

- To display the keyboard logger audit log file, use the following command:

```
seaudit -kbl -a -sid 22764
```

- To replay a user session, use the following command:

```
seaudit -kbl -sid 22316 -rp
```

- To display all the commands that a user enters in a session, use the following command:

```
seaudit -kbl -sid 22316 -cmd
```

- To list all audit records that trace the activity of a single user with UID 244 attempting to access files, use the following command:

```
seaudit -tru 244 -trr FILE
```

- To list all audit records that trace the activity of two users, use the following command:

```
seaudit -tru "user1, 244"
```

- To list all audit records logged from 5 minutes ago, use the following command:

```
# date
Fri Nov 25 01:50:00 EST 2016

# /opt/CA/PAMSC/bin/seaudit -a -st now-5
CA Privileged Access Manager Server Control seaudit <version> - Audit log lister
Copyright (c) 2013 CA. All rights reserved.
25 Nov 2016 01:45:00 P FILE root Read 54 2 /etc/security/passwd /usr/sbin/cron root
25 Nov 2016 01:45:00 P FILE root Read 54 2 /etc/security/passwd /usr/sbin/cron root
25 Nov 2016 01:45:00 P FILE root Read 54 2 /etc/security/passwd /usr/sbin/cron root
25 Nov 2016 01:45:00 P LOGIN root 59 2 _CRONJOB_ USR_SBIN_CRON
25 Nov 2016 01:45:00 P FILE root Read 54 2 /etc/security/passwd /usr/sbin/cron
_CRONJOB_ root
```

```
25 Nov 2016 01:45:00 O LOGOUT root 49 2 _CRONJOB_
```

```
Total records displayed 6
```

## sebuildla Utility Create a Lookaside Database

### Valid on UNIX

The `sebuildla` utility creates a lookaside database for use by the Privileged Access Manager daemon, `seosd`. The `seosd` daemon uses the database to translate UNIX UIDs to user names, GIDs to group names, host IP addresses to host names, and service ports to port names. The database contains only the number to name translation. `sebuildla` also lets you add information from the LDAP Directory Information Tree (DIT) to the user lookaside database.

#### WARNING

To set up `sebuildla` and the required LDAP configuration settings, you must be familiar with LDAP and must be able to execute the `ldapsearch` command. We recommend that you read the man pages for `ldap(1)`, `ldapsearch(1)`, and the information about setting up in the documentation for your LDAP client. Also, before you use `sebuildla` to build the lookaside databases, specify the full path of the lookaside database, in the `lookaside_path` configuration setting.

The first time that you build the lookaside database, use the following command:

```
sebuildla -a
```

This creates *all* of its components. Single files of the database can be updated later by using the relevant switches.

If you installed Privileged Access Manager on a NIS, NIS+, or DNS server, place calls to the `sebuildla` utility in the related makefiles.

#### NOTE

By default, the lookaside database files (`groupdb.la`, `hostdb.la`, `servdb.la`, and `userdb.la`) are protected against all user access other than access with the `sebuildla` program.

The `sebuildla` utility scans the resolution mechanisms in the system, such as `/etc` files and NIS, to build the lookaside databases.

- `sebuildla` reads `/etc/resolv.conf` to get the domain name used.

#### NOTE

For Privileged Access Manager to resolve host names to fully qualified names, the `resolv.conf` file must have either the domain or search configuration option defined. For more information about the `resolv.conf` file, see the man pages for this file.

- `sebuildla` uses the system resolution option to create the lookaside database. (This is usually the net caching daemon.)
- Privileged Access Manager uses the `/etc/nsswitch.conf` file (for the net caching daemon or any other system resolution option) to decide where to retrieve data from.

For example, if the `/etc/nsswitch.conf` file contains the following line for hosts, information is retrieved from the local machine's files first (`/etc/hosts`); it then retrieves information from the DNS and then the NIS:

```
hosts:      files dns nis
```

If the file contains the following line instead, information is retrieved only from your local machine's files. The look aside database contains only the hosts that are in `/etc/hosts`:



hosts:            files

## NOTE

If a host has a fully qualified name, sebuildla uses it.

Variations in machine configuration may cause instances where sebuildla does not list all the names of a local environment. In this case, you can use sebuildla to load all the required entries from a list file. To do this, create a list file with each object name on a separate line. The utility reads this list file and ensures that all the objects in the list file are added to the relevant lookaside database if necessary. sebuildla ignores duplicate objects.

The following table lists the files sebuildla uses to build each lookaside database.

Objects in	Are added to the
<i>ACInstallDir</i> /ladb/userlist	users lookaside database
<i>ACInstallDir</i> /ladb/grouplist	groups lookaside database
<i>ACInstallDir</i> /ladb/hostlist	hosts lookaside database
<i>ACInstallDir</i> /ladb/servlist	services lookaside database

In the format of the files in the *ACInstallDir*/ladb directory:

- sebuildla ignores empty lines or lines that begin with an exclamation point (!), number sign (#), or a semicolon (;).
- Other lines represent entries that sebuildla must add to the appropriate lookaside database, if the entry can be resolved.
- The user, group, host, or service name must start in the first position of the line.

You can use dbmgr -dump -r 1 HOST > /opt/CA/PAMSC/ladb/hostlist to create the list files. For example, to create a list of the hosts that are defined in class HOST in the local database, enter:

```
dbmgr -dump -r 1 HOST > /opt/CA/PAMSC/ladb/hostlist
```

The -l switch makes a single request from DNS for a list of all hosts in the default domain, instead of querying the DNS server for the FQDN of each host entry as it is obtained. The fast load option is effectual only if DNS is installed. Only host names in the default domain are made fully qualified. Fully qualified names are left as such. Host names that are scanned from the system mechanism that are not fully qualified, and are not found in the default domain, are left unqualified. Host names that are loaded from the hostlist file that are not fully qualified are discarded.

This command has the following format:

```
sebuildla switch [options]
```

- **switch**  
Specifies the mode of operation for the utility. Can be *one* of the following:
  - **-a**  
Creates *all* the lookaside database files.
  - **-e**  
Creates a hosts lookaside database file excluding the DNS.
  - **-g**  
Creates a groups lookaside database file.
  - **-h**

Creates a hosts lookaside database file with the DNS.

– **-help**

Displays the help for this utility.

– **-n**

Collects information from an LDAP Directory Information Tree (DIT) and appends it to the users lookaside database it creates from the primary user data source (-u switch). You can only use this switch with the -u switch or the -a switch so it is most useful when the LDAP DIT provides more user data and is not used as the system's naming service.

Before you use this switch, follow these steps:

- a. Set the following seos.ini file tokens for Privileged Access Manager to find the LDAP service: ldap\_base, ldap\_hostname, and ldap\_userdn
- b. Run the seldapcred utility to store the encrypted LDAP password.
- c. (Optional) Set the ldap\_port and ldap\_timeout tokens for your environment.  
The time it takes to retrieve information from the LDAP service depends on how fast the LDAP service is, and how much user data is stored in the DIT. You can adjust the ldap\_timeout token in the [seos] section of the seos.ini file to account for these aspects.
- d. (Optional) If you are using a non-standard schema, set the ldap\_uid\_attr, ldap\_uidNumber\_attr, and ldap\_user\_class tokens.

– **-s**

Creates a services lookaside database file.

– **-u**

Creates a users lookaside database file.

**NOTE**

You can specify the -n switch with the -u switch to add user data that is collected from an LDAP service.

– **-G**

Lists the contents of the groups lookaside database files.

– **-H [IPv4 | IPv6]**

Lists the contents of the hosts lookaside database files.

– **-S**

Lists the contents of the services lookaside database files.

– **-U**

Lists the contents of the users lookaside database files.

• *options*

Specifies optional modifiers that change the way that the utility displays its information. Can be one or more of the following:

– **-l**

Loads the lookaside database using only the list file. This excludes the resolution mechanism of the system.

– **-f**

Fast loads the lookaside database (hosts only) when using the -h switch.

## sechkey Utility

Use the sechkey utility to manage Privileged Access Manager encryption and so protect your Privileged Access Manager management communications. You must have the ADMIN attribute to use sechkey.

You can use it to set an encryption key for symmetric encryption, or you can use it for SSL (PKI) encryption.

If you are using symmetric keys, we recommend that you change the key from the default. If you are using SSL, we recommend that you change the default certificate and associated private key from the default.

Whichever encryption method you use, change the keys on all computers at your site after you have installed or upgraded Privileged Access Manager. This prevents unauthorized users from accessing the system.

The utility handles the following tasks:

- [Change a symmetric encryption key](#)
- [Change the symmetric encryption method](#)
- [Configure X.509 certificates](#)

## sechkey Utility Change a Symmetric Encryption Key

The sechkey utility changes the Privileged Access Manager symmetric encryption key for Privileged Access Manager programs.

You can run sechkey in interactive or non-interactive mode. When you run sechkey in interactive mode, sechkey prompts you to enter the old and new encryption keys.

You must stop Privileged Access Manager before you use sechkey to change a symmetric encryption key. You must have the ADMIN attribute to use sechkey.

### WARNING

To avoid communication problems, use the same encryption key on all computers that run Privileged Access Manager components.

This utility has the following format in interactive mode:

```
sechkey
```

This utility has the following format in non-interactive mode:

```
sechkey {oldkey | -d} {newkey | -d} [-s registry_path]
```

sechkey has some additional switches that are only valid on UNIX computers. This utility has the following format for UNIX computers:

```
sechkey {oldkey | -d} {newkey | -d | -n} [-nopmd | -r hostname]
```

```
sechkey -k newkey
```

```
sechkey -c
```

- **-c**  
(UNIX) Clears the selogrd encryption key. The default key is saved in the key file.  
**Note:** The saved key itself is encrypted with the default encryption method.
- **-d**  
Specifies the default Privileged Access Manager key.
- **-k**  
(UNIX) Specifies the selogrd encryption key that you want to change to. The encryption key is saved in a new file or updated in the old one.
- **-n**  
(UNIX) Lists the programs that are using the current key, without changing to a different key.
- *newkey*  
Specifies the new encryption key.
- **-nopmd**  
(UNIX) Changes the key without updating the Policy Model update file with the new key.
- *oldkey*  
Specifies the (current) encryption key that you want to change.
- **-r hostname**  
(UNIX) Specifies the name of the remote computer whose encryption key you want to change.

To use this option, Privileged Access Manager must be running on both the local and remote computers. This parameter does not actually change the key; rather, it saves information so that the next time you start Privileged Access Manager on the remote computer (using `seload -c`), the key is changed.

- **-s *registry\_path***  
(Windows) Specifies the registry root path where the encryption key for Privileged Access Manager programs is stored. This switch is only valid for third-party programs that use the Privileged Access Manager SDK.

### Example: Check If a UNIX Computer Uses the Default Encryption Key

The following command checks if a UNIX computer uses the default Privileged Access Manager encryption key:

```
sechkey -d -n
```

### sechkey Utility Change the Symmetric Encryption Method

The `sechkey` utility changes the symmetric encryption method for Privileged Access Manager programs. When you change the symmetric encryption method, `sechkey` decrypts each encrypted password in the Privileged Access Manager database then encrypts each password with the new encryption method.

#### NOTE

If Privileged Access Manager is operating in FIPS-only mode, you cannot change the symmetric encryption method. Privileged Access Manager operates in FIPS-only mode when the value of the `fips_only` configuration token in the `crypto` section is 1. This restriction prevents you from changing the encryption method to a non-FIPS compliant method.

You must stop Privileged Access Manager before you use `sechkey` to change the symmetric encryption method. You must have the ADMIN attribute to use `sechkey`.

#### WARNING

To avoid communication problems, use the same encryption method on all computers that run Privileged Access Manager components.

This utility has the following format:

```
sechkey -m -sym {aes128 | aes192 | aes256 | des | tripledes | default} [-s registry_path]
```

- **-m**  
Specifies to change the encryption method.
- **-s *registry\_path***  
(Windows) Specifies the registry root path where the encryption key for Privileged Access Manager programs is stored. This switch is only valid for third-party programs that use the Privileged Access Manager SDK.
- **-sym**  
Specifies the new encryption method to use.
  - **aes128**  
Specifies to use the following encryption method:  
(Windows): `aes128enc.dll`  
(UNIX): `libaes128.so`
  - **aes192**  
Specifies to use the following encryption method:  
(Windows): `aes192enc.dll`  
(UNIX): `libaes192.so`
  - **aes256**  
Specifies to use the following encryption method:  
(Windows): `aes256enc.dll`  
(UNIX): `libaes256.so`
  - **des**

Specifies to use the following encryption method:

(Windows): desenc.dll

(UNIX): libdes.so

– **tripleDES**

Specifies to use the following encryption method:

(Windows): tripledesenc.dll

(UNIX): libtripleDES.so

– **default**

Specifies to use the following proprietary Privileged Access Manager encryption method:

(Windows): defenc.dll

(UNIX): libscramble.so

### Example: Change the Symmetric Encryption Method to AES256

The following command changes the symmetric encryption method to AES256:

```
sechkey -m -sym aes256
```

### sechkey Utility Configure X.509 Certificates

The sechkey utility configures the root and server certificates that Privileged Access Manager uses to authenticate communication between components.

You can use the sechkey utility to perform the following tasks:

- Configure Privileged Access Manager to use third-party root and server certificates, including OU password-protected certificates
- Create a server certificate from a third-party root certificate
- Save the password of a password-protected certificate on the computer

Stop Privileged Access Manager before you use sechkey to configure X.509 certificates. You must have the ADMIN attribute to use sechkey.

#### NOTE

If Privileged Access Manager is operating in FIPS-only mode, you cannot use password-protected certificates. Privileged Access Manager operates in FIPS-only mode when the value of the `fips_only` configuration token in the `crypto` section is 1. This restriction prevents you from encrypting passwords within the certificate with a non-FIPS compliant method.

This command has the following format to create an X.509 root or server certificate:

```
sechkey -e {-ca|-sub [-priv privfilepath]} [-in infilepath] [-out outfilepath] [-capwd password] [-subpwd password]
```

This command has the following format to use OU password-protected server certificates:

```
sechkey -g {-subpwd password | -verify}
```

- **-ca**

Specifies that sechkey creates a self-signed certificate that is used as a CA (root) certificate.

sechkey stores the certificate and private key in the PEM file that is defined by the `ca_certificate` configuration setting in the `crypto` section.

- **-capwd password**

Specifies the password for the private key of the root certificate that sechkey uses to generate a server (subject) certificate.

- **-e**  
Specifies that sechkey creates an X.509 certificate.
- **-g**  
Specifies that Privileged Access Manager uses third-party server certificates. Save the third-party server certificate in the location that is specified in the `subject_certificate` configuration setting in the `crypto` section. you can also edit the value of the `subject_certificate` configuration setting in the `crypto` section to specify the full path to the third-party server certificate.

#### NOTE

If you install the server certificate in a new directory, write Privileged Access Manager FILE rules to protect the new directory.

- **-in *infilepath***  
Specifies the input file that contains the certificate information. If `-in` is not specified, sechkey reads the information from the standard input.  
sechkey requires the following information to create a certificate:
  - Serial Number
  - Subject
  - Not Before (First valid day for certificate)
  - Not After (Last valid day for certificate)
 sechkey can use the following information, but the information is not mandatory:
  - Email
  - URI (often named URL)
  - DNS name
  - IP Address
- **-out *outfilepath***  
Specifies the output file to put the certificate information. The output file is a copy of the input information. If `-out` is not specified, sechkey does not duplicate the input information.
- **-priv *privfilepath***  
Specifies the file that holds the private key that is associated with the certificate. This option is only valid when used with the `-sub` option.
- **-sub**  
Specifies that sechkey creates a server (subject) certificate.  
sechkey stores the certificate and private key in the PEM file that is defined by the `subject_certificate` configuration setting in the `crypto` section.  
If `-priv` is not specified, the `private_key` configuration setting in the `crypto` section defines the file that holds the private key that is associated with the certificate.  
If you create a password-protected server certificate, sechkey does not encrypt the certificate. If you create a server certificate that is not password-protected, sechkey encrypts the certificate using AES256 and the Privileged Access Manager encryption key.
- **-subpwd *password***  
Specifies the password for the private key of the server (subject) certificate. sechkey stores the password in the `crypto.dat` file in the `ACInstallDir/Data/crypto` directory, where `ACInstallDir` is the directory in which you installed Privileged Access Manager. The `crypto.dat` file is hidden, encrypted, read-only, and protected by Privileged Access Manager. Privileged Access Manager is stopped, only the superuser can access the password.
- **-verify**  
Verifies that Privileged Access Manager can use the stored password to open the password-protected server key.

**Example: Create a Server Certificate from an OU Password-Protected Third-Party Root Certificate**

The following command creates a server certificate from an OU password-protected third-party root certificate, using the following values:

- The path to the input file that contains the certificate information is C:\Program Files\CA\PAMSC\data\crypto\sub\_cert\_info
- The path to the private key for the root certificate is C:\Program Files\CA\PAMSC\data\crypto\ca.key
- The password for the private key for the root certificate is P@ssw0rd

```
sechkey -e -sub -in "C:\Program Files\CA\PAMSC\data\crypto\sub_cert_info" -priv "C:\Program Files\CA\PAMSC\data\crypto\ca.key" -capwd P@ssw0rd
```

### Example: Input File

The following is an example of an input file that contains certificate information with IPv4 addresses:

```
SERIAL: 00-15-58-C3-5E-4B

SUBJECT: CN=192.168.0.1

NOTBEFORE: "12/31/08"

NOTAFTER: "12/31/09"

E-MAIL: john.smith@example.com

URI: http://www.example.com

DNS: 168.192.0.100

IP: 168.192.0.1
```

For IPv6, the DNS and IP addresses are shown below:

```
...
DNS: fd6d:8d64:af0c:1:0:242:22:233
IP: ssl://[fd6d:8d64:af0c:1:0:242:22:233]:61616
```

## seclassadm Utility Administer CA Privileged Access Manager Server Control Classes

The seclassadm utility manages Privileged Access Manager classes. The utility adds new user-defined classes to the local database. Invoke it from the directory in which the database resides (or use the -p option), while Privileged Access Manager is *not* running.

### NOTE

Running seclassadm creates a file in the seosdb directory with the new class information. When you create a new database with dbmgr -c, user-defined classes are created in the new database if the CreateNewClasses configuration setting is set to yes (the default).

This command has the following format:

```
seclassadm -add className [-a access] [{-|+}c] [-d access] \
```

```
[-f] [-g] [-o] [-p db_pathname] [-t]
seclassadm -del className
seclassadm -upd className {-|+}c [-p db_pathname]
```

- **-add *class-name***  
Adds a new resource class to an existing database, where *class-name* is the name of the new class. Privileged Access Manager reserves class names that are in uppercase characters. When adding a class, use at least one lowercase character. Class names can be up to 79 characters long. After creating a class, enable the class by using the selang setoptions command.
- **-del *class-name***  
Deletes the specified resource class from the database.
- **-upd *class-name***  
Updates the specified resource class in the database.
- **-a *access***  
Specifies the access modes for the class. The string *access* represents the allowed accesses. A single character code that is listed in any order represents each access mode. The string must not contain any blank or other non-alphabetic characters. Valid access modes are:

Abbreviation	Description
C	control
D	delete
E	create
F	filesan
M	chmod
O	chown
R	read
S	security
T	utime
U	update
V	rename
W	write
X	execute

- **-d *access***  
Specifies the default access mode for the class. This is the access mode that Privileged Access Manager assigns to a user when you execute the authorize command without specifying an access authority. This implicit access that is used by the authorize command is *not* the same as the default access assigned to a resource. The possible accesses modes are listed in the -a option.
- **-f**  
Specifies that Privileged Access Manager accepts a new class name, even if the name contains all uppercase letters.

**NOTE**

By default, the seclassadm utility does not let you create a class name that is all uppercase. Privileged Access Manager uppercase names are reserved for the predefined Privileged Access Manager classes.

- **-g**  
Specifies that the new class is a resource that groups members of an existing class. The relationship between the existing class and the new group class is the same as the relationship between any class and its group class in the



database (for example, `TERMINAL` and `GTERMINAL`). A resource that groups members of an existing class must begin with the uppercase letter `G`. That is, it has the same name as the existing class, but begins with the prefix `G`.

- **-o**  
Creates a `_default` record for the new class and sets its default access.
- **-p *db\_pathname***  
Specifies the full pathname of the local database.  
By default, the utility works on the database in the current directory. Use this option to define a different directory where the database resides.

### Examples: Add a new class to the database

The following examples demonstrate how you can use the `seclassadm` utility to add a class to the database:

- To add a resource class by the name *dbfield*, use the following command:  

```
seclassadm -add dbfield
```
- To add a resource class by the name *report* with only `READ` access, use the following command:  

```
seclassadm -add report -d R -a R
```
- To add a resource class by the name *batch\_jobs* with `READ`, `WRITE`, and `MODIFY` permissions and `READ` access as the default when not specified, use the following command:  

```
seclassadm -add batch_jobs -d R -a RWM
```
- To add a new class whose objects are groups of resources in the class `DEPTA`, with access `execute` and implicit access `execute`, use the following command:  

```
seclassadm -add DEPTA -d X -a X -g -f
```

## secompas Utility Compare Passwords

### Valid on UNIX

The `secompas` utility compares passwords in the Privileged Access Manager database with the passwords in the UNIX password file.

For each user in the Privileged Access Manager database, the utility outputs one line that contains the user name and a message indicating whether the user is not defined in UNIX, whether the user has no password in Privileged Access Manager, or whether the passwords match. The utility also displays the total number of users it compared and the number of users whose passwords do not match. It only adds to this total when the password exists in both environments and it is not the same. If a user is not defined in an environment, or the password is missing from an environment, `secompas` does not add to the counter of unmatched passwords.

To compare passwords, the `secompas` utility uses the `/etc/passwd` file, the shadow password files, and NIS/NIS+ password maps.

### NOTE

You must have the `ADMIN` attribute to use this utility.

This command has the following format:

```
secompas [-db] [-ok] [-ux]
```

- **-db**  
Specifies not to display users that do not have a password in the Privileged Access Manager database.
- **-h**  
Displays the help for this utility.
- **-ok**  
Specifies not to display users that have the same password in the Privileged Access Manager database and UNIX (password match).
- **-ux**

Specifies not to display users that do not exist in UNIX.

### Example: Utility output

This example shows sample output from the utility:

```
Checking root           : No password in Access Control database.
Checking tst_001       : Undefined in UNIX.
Checking tst_002       : No password in UNIX password file
Checking tst_003       : *** PASSWORDS DO NOT MATCH. ***
Checking tst_004       : *** NO MATCH - UNIX DISABLED ***
Checking tst_005       : OK
```

Total of 6 users found in database.

2 unmatched password(s) found. (1 UNIX DISABLED).

The following explains each line in the preceding output:

```
Checking root           : No password in Access Control database.
```

Either the user *root* is not defined in the Privileged Access Manager database or the user is defined in the database but does not have a password in it.

```
Checking tst_001       : Undefined in UNIX.
```

The user *tst\_001* is defined in the Privileged Access Manager database but not in UNIX.

```
Checking tst_002       : No password in UNIX password file
```

The user *tst\_002* is defined in UNIX but does not have a password.

```
Checking tst_003       : *** PASSWORDS DO NOT MATCH. ***
```

The Privileged Access Manager password does not match the UNIX password of the user *tst\_003*.

```
Checking tst_004       : *** NO MATCH - UNIX DISABLED ***
```

The *tst\_004* user account was disabled in the UNIX environment. *secompas* identifies a disabled user account by the asterisk (\*) in front of the password in the */etc/passwd* file.

```
Checking tst_005       : OK
```

The Privileged Access Manager password matches the UNIX password of the user *tst\_005*.

## secons Utility

The *secons* utility is the Privileged Access Manager security console. It lets you perform the following tasks:

- On UNIX:

- Display run-time statistics on Unix
- [Manage concurrent login options](#)
- Manage Privileged Access Manager tracing
- [Manage Enabled Kernel](#)
- [Manage resource caching](#)
- [Manage CA Privileged Access Manager Server Control shutdown](#)
- [Reload configuration settings](#)
- [Remove XUSER objects](#)
- [Display kernel tables](#)
- [Clean, enable, or disable kernel cache tables](#)
- On Windows:
  - [Control instrumentation run-time settings](#)
  - [Display run-time statistics on Windows](#)
  - [Display ACEE Records](#)
  - [Manage concurrent login options](#)
  - Manage Privileged Access Manager tracing
  - [Refresh IP addresses for network resources](#)
  - [Remove XUSER objects](#)
  - [Resolve recycled accounts](#)
  - [Shut down CA Privileged Access Manager Server Control](#)
  - [Display your user name and security credentials](#)

The secons utility is available to both security administrators and other users. However, only some options are available for users who do not have the ADMIN attribute. These options are:

-m (trace management), -d-, -d+, -ds (login management), and -whoami (user's credentials).

## secons Utility Manage CA Privileged Access Manager Server Control Shutdown on UNIX

### Valid on UNIX

The secons utility shuts down Privileged Access Manager and the associated daemons. You can also use this utility to find out which processes are still executing Privileged Access Manager code.

Only users who are defined as ADMIN or OPERATOR can shut down Privileged Access Manager. To shut down Privileged Access Manager on remote computers, you must be defined as ADMIN or OPERATOR on those remote computers.

This command has the following format:

```
secons [-s [hosts | ghosts]] \
      [-S [{selogrd | selogrcd | serevu}]] \
      [-sc] [-scl] [-sk]
```

- **-s [hosts | ghosts]**  
Shuts down the Privileged Access Manager daemons on the defined, space-separated, list of remote hosts. If you do not specify any hosts, Privileged Access Manager shuts down on the local host.

You can define a group of hosts by entering the name of a *ghost* record. If you use this option from a remote terminal, the utility requests password verification. You also need admin privileges on both the remote and local computers, and write permission to the local computer on the remote host database.

- **-S [{selogrd | selogrcd | serevu}]**

If you do not define a daemon, terminates the Privileged Access Manager daemons and attempts to terminate active daemons selogrd, selogrcd, and serevu. If the selogrd, selogrcd, or serevu tokens in the [daemons] section of seos.ini file are set to *yes*, termination request is sent to the running Privileged Access Manager main daemon or a termination signal is sent to the specified daemon if the product is already down.

If you define a daemon, secons does not terminate the Privileged Access Manager daemons. If the appropriate token in the [daemons] section of seos.ini file is set to *yes*, it sends the termination request to the running Privileged Access Manager main daemon or it sends the termination signal to that daemon if Privileged Access Manager is down.

- **-sc[l]**

Displays processes that are still executing Privileged Access Manager code.

You cannot unload Privileged Access Manager if an application, which is loaded on top of Privileged Access Manager, has an open system call (syscall) that is hooked by Privileged Access Manager. Once you know which processes are still executing Privileged Access Manager code, you can shut down these processes and can unload the Privileged Access Manager kernel module. You can then use UNIX exits to automatically shut down these processes before unloading the kernel and then restart them after the kernel unloaded.

The *-sc* output displays as a two-column table with the system call number in the first column, and the process identifier in the second column.

The *-sc/* option also displays parent process ID (PPID), UID, time, and program name information for the processes that are still executing Privileged Access Manager code. The time information lets you find out how long the process has Privileged Access Manager hooked. If the time is relatively short, the hook is likely to be a temporary one.

You can also run this while Privileged Access Manager is running to help you predict what causes unload issues in advance. However, sometimes, such as the *accept* command, Privileged Access Manager code removes the hook during unload. This means that some of the active hooks you see while Privileged Access Manager is running may not actually affect unloading.

**Note:** By default, Privileged Access Manager monitors system calls that it intercepts. Set the *syscall\_monitor* token in the seos.ini file to 0 (disabled) if you do *not* want Privileged Access Manager to monitor system calls.

- **-sk**

Shuts down all Privileged Access Manager daemons and prepares the Privileged Access Manager kernel extension to be unloaded.

### Example: Shut Down Privileged Access Manager

- To shut down the Privileged Access Manager daemon, enter:

```
secons -s
```

- To shut down the Privileged Access Manager daemon on remote hosts HOST1 and HOST2, enter:

```
secons -s HOST1 HOST2
```

### Example: Display Information for Processes that are Still Executing Privileged Access Manager Code

- To display basic information about processes that are still executing Privileged Access Manager code:

```
secons -sc
```

The output that you receive looks similar to the following:

```
CA PAMSC secons vX.X.X.xxx - Console utility
```

```
Copyright (c) YYYY CA. All rights reserved.
```

```
Active system calls:
```

```
syscall      5 - PID: 27477
```

- To display more information about processes that are still executing Privileged Access Manager code:

```
secons -scl
```

The output you receive looks similar to the following:

```
CA PAMSC secons vX.X.X.xxx - Console utility
```

```
Copyright (c) YYYY CA. All rights reserved.
```

```
Active system calls:
```

```
-Syscall 102 - PID: 2105 PPID: 1 UID: 0 TIME: 4d-4h PROGRAM NAME: /usr/sbin/vsftpd
```

```
Syscall 5 - PID: 24269 PPID: 4289 UID: 0 TIME: 2d-21h PROGRAM NAME: /bin/bash
```

A dash (-) at the beginning of the output line means that Privileged Access Manager assesses that this hook is not likely to cause you issues when unloading. When you use this command, Privileged Access Manager also adds lines to the audit log that records whether the unloading Privileged Access Manager is likely to succeed. For example, the following audit record is created when you run `secons -scl` and there is at least one blocking system call that is likely to prevent Privileged Access Manager from unloading:

```
10 Nov YYYY 05:47:22 F CHECK      root      Scan      339 0 SEOS_syscall      unload
```

## secons Utility Manage CA Privileged Access Manager Server Control Tracing

The `secons` utility manages Privileged Access Manager tracing. Tracing lets you monitor operating system events. Privileged Access Manager can accumulate a file of messages reporting operating system events that you can then display.

This command has the following format:

```
secons [-t+] [-t-] [-tt] [-ts] [-tc] [-tv [size] [-file fileName]]
secons -m message
secons -send heartbeat
secons -pupm trace {enable | disable | clear}
```

- **-m *message***  
Adds a text message to the trace file.
- **-t+**  
Enables tracing, which causes the Privileged Access Manager engine (`seosd`) to dump messages that specify its operations and actions to the trace file.
- **-t-**  
Disables tracing, which stops the Privileged Access Manager engine `seosd` from dumping messages to the trace file.
- **-tc**  
Clears the trace file, removing all records from it.

**NOTE**

You can use this option whether seosd is running.

- **-ts**  
Displays the current tracing status.
- **-tt**  
Toggles the tracing status.
- **-tv [size] [-file fileName]**  
Displays a real-time trace output. The utility displays the last *size* KB (by default, 2 KB) of the trace file and keeps the session open so that any new trace messages added to the file are displayed. This is similar to the UNIX tail -f command.  
Use Ctrl+C to stop this operation.  
**Note:** You can use this option whether seosd is running. Use the full\_year configuration setting to select whether you want to display the year in four digits (the default, yes) or two digits.
  - *size*  
Specifies the size, in kilobytes, of the portion of the file you want to display, starting from the end. Specify 0 to show the entire trace file. If you do not specify this option, secons uses the default, 2 KB.
  - *-file fileName*  
Reads *fileName* instead of *ACInstallDir/log/seosd.trace*.
- **-send heartbeat**  
Sends a heartbeat to the Privileged Access Manager Server immediately.
- **-pupm trace {enable | disable | clear}**  
**Valid for the Shared Account Management Agent**  
Specifies tracing options on the Shared Account Management Agent during runtime. You do not need to restart Privileged Access Manager to modify the trace options.  
**Limits:** enable, enables tracing; disable, disables tracing; clear, clears the trace file.

**WARNING**

The trace options that you specify apply to the current session only. After Privileged Access Manager restarts the trace option is set according to the OperationMode token in the PUPMAgent section.

## secons Utility Manage Concurrent Login Options

The secons utility manages concurrent login options. You can configure Privileged Access Manager to prevent a user from logging in more than once. This prevents intruders from logging into the accounts of users who are already logged in.

This command has the following format:

```
secons [-d+] [-d-] [-ds] [-l+] [-l-] [-ls] \
      [-u+ userName] [-u- userName] [-us userName]
```

- **-d+**  
Enables concurrent logins for the user running the command.
- **-d-**  
Disables concurrent logins for the user running the command. Using this command kills any concurrent logins of the user to the local computer.

**NOTE**

You can also place this command in the .login or .cshrc file of a user to disable concurrent logins.

- **-ds**  
Displays the concurrent logins setting for the user running the command.
- **-l+**  
Enables concurrent logins system-wide.

**NOTE**

By default, Privileged Access Manager enables login, but in cases where the system is shut down for maintenance, you can disable login for a specific period.

- **-l-**  
Disables concurrent logins system-wide.
- **-ls**  
Displays system-wide login status.
- **-u+ *userName***  
Enables concurrent logins for the defined user.
- **-u-*userName***  
Disables concurrent logins for the defined user.
- **-us *userName***  
Displays the concurrent logins setting for the defined user.

## secons Utility Manage Resource Caching on UNIX

### Valid on UNIX

The secons utility manages resource caching (file cache) on UNIX. The cache, a runtime table, "remembers" the previous answer to an authorization request (permit or deny) for resources in the FILE class. When an identical authorization is requested, the request is answered with the last response that was stored in the cache memory tables.

This command has the following format:

```
secons [-C+] [-C-] [-CA value] [-CC interval] [-CD] \
[-CF value] [-CI init_value] [-CP interval] -CU value]
```

- **-C+**  
Enables caching of file authorization.
- **-C-**  
Disables caching of file authorization.
- **-CA *value***  
Specifies the maximum number of authorization records in a table.  
**Default:** 80  
**Limits:** A number between 1 and 800
- **-CC *interval***  
Specifies the cache clean interval in minutes.  
**Default:** 60  
**Limits:** A number greater than 0
- **-CD**  
Displays the cache table to the standard output.
- **-CF *value***  
Specifies the maximum number of file records in a table.  
**Default:** 20  
**Limits:** A number between 1 and 200
- **-CI *init\_value***  
Specifies the initial priority value for a new record in the cache table.  
**Default:** 10
- **-CP *interval***

Specifies the cache priority computing interval.

**Default:** 1 (one record)

**Limits:** A number between 1 and 10

- **-CU value**

Specifies the maximum number of user records in a table.

**Default:** 50

**Limits:** A number between 1 and 500

### Example: Change cache settings

The following example shows you how you can change settings of the cache so that the maximum number of file, user, and authorization records in the cache are 60:

```
secons -CF 60 -CU 60 -CA 60
```

### Example: Display the cache table

The following example shows the output of the secons -CD command:

```
=====
FILE CACHE (configuration, statistics, and dispatcher data)
=====
sizes(bytes)      tables:          | max records:      | intervals
cache  head      files    users    auth | files users auths | clean prio
-----
40244   44        5600    4200    30400 | 20   50   80   | 60  1
=====
table |statistics          | priority  |min | rec | average      |pri |init
name  | hits misses (ok) | maxim  minim|ind | used | usage  life |fact|prio
-----
files |   5   1  83% |   0     0 | 0 | 1 |         |    | 
users |   5   1  83% |  10     2 | 0 | 1 | 0       | 0  | 1 | 10
auths |   4   2  66% |   2     | 0 | 2 |         |    | 
=====
FILE TABLE
=====
No  type    pid priority user                                file name
-----
0   EXPL    372      0   0                                /etc/shadow
=====
USER TABLE
=====
No  user name    prio  life  used  UID  EUID  RUID  auth prev(file)next
-----
0   root        2     2    7    0    0    0    0    50( 0) 50
=====
AUTHORIZATION RESULT TABLE (R - Result: 'P'-permit, 'D'-deny ...)
=====
No  R ACEE acc  Log stage prv(usr)nxt time          terminal  program
-----
0   P   6  read  0  00036 80( 0) 1   07:48:25          /usr/bin/login
=====
```

The following explains the preceding output:

The output consists of five parts:



- The cache configuration. It contains the following fields:
  - Size of the cache (in bytes)
  - Size of the cache header (in bytes)
  - Size of the file table (in bytes)
  - Size of the user table (in bytes)
  - Size of the results table (in bytes)
  - The maximum number of file records
  - The maximum number of user records
  - The maximum number of result records
  - Statistic: hits in the table
- The table of file records. It contains the following fields:
  - Sequential number of the record
  - Type of the file (EXPLICIT, IMPLICIT)
  - Process ID number
  - Priority of the record, is sum of its users priorities
  - Appropriate user record number in the table of users
  - Name of the file
- The table of users. It contains the following fields:
  - Sequential number of the record
  - User name
  - Priority of the record
  - Record lifetime counter
  - Record usage counter
  - User ID; user effective ID; really used by security ID
  - Appropriate authorization record number in the table of authorization
  - Previous user record number in the chain of users
  - Appropriate file record number
  - Next user record in the chain of users
- The table of authorization results. It contains the following fields:
  - Terminal
  - Stage
  - Granted stage
  - Result - authorization result (P or D)
  - ACEE number
  - Access type
  - Logging options flag value
  - The stage number the decision was made
  - Previous authorization record number in the chain of records
- Appropriate user record number
  - Next authorization record number in the chain of records
  - Statistic: the number of missed records in the table
  - Authorization class
  - Program name (with the via parameter)
  - Notification string
  - Update time (GMT)
- Dispatcher Data. It contains the following fields:

- Statistic: number of missed records in the table
- Statistic: number of hits in the table
- Maximum priority in a table
- Minimum priority in a table
- Number of entries with minimum priority
- Number of used records
- Average usage (only for users table)
- Average life (only for users table)
- Priority calculation factor (only for users table)
- Initial value of the record priority (only for users table)

## secons Utility Shut Down Privileged Access Manager Server Control on Windows

### Valid on Windows

The secons utility shuts down the Privileged Access Manager engine and all other Privileged Access Manager services on the local station or on one or more remote stations.

Only users defined as ADMIN or OPERATOR can shut down Privileged Access Manager. To shut down Privileged Access Manager on remote computers, you must be defined as ADMIN or OPERATOR on those remote computers.

This command has the following format:

```
secons -s [hosts | ghosts]
```

**-s** [*hosts* | *ghosts*]

Shuts down the Privileged Access Manager services on the defined, space-separated, remote hosts. If you do not specify any hosts, Privileged Access Manager shuts down on the local host.

You can define a group of hosts by entering the name of a ghost record. If you use this option from a remote terminal, the utility requests password verification. You also need admin privileges on both the remote and local computers, and write permission to the local computer on the remote host database.

## secons -dbclean Remove XUSER Objects from the CA Privileged Access Manager Server Control Database

The secons utility removes XUSER objects that were not resolved to their native security identifiers (SID) from the Privileged Access Manager database. Use the secons -dbclean command to remove XUSER objects that no longer exist in the native environment.

This command has the following format:

```
secons -dbclean <osuser>
```

- **-dbclean**  
Specify to remove all XUSER objects that were not resolved from the Privileged Access Manager database.
- **<osuser>**  
Specifies the native user account name.

## secons -acee Function Display ACEE Records on Windows

### Valid on Windows

The `secons` utility lets you monitor the Accessor Element Entry (ACEE) table that caches accessors in the authorization engine. The ACEE stores information about the following users:

- **Logged in user** A user that has logged in to the operating system. Specific ACEE attributes for this type of user are:
  - Login session ID
  - Login session type
- **Management user** A user that has logged in to a Privileged Access Manager management application (using an LCA connection). For example, `selang`.
- **Authorization API user** A user that was referenced in `SEOSROUTE_*` API.
- **SPECIALPGM Logical user** A user that is being referenced at least in one SPECIALPGM record. A specific ACEE attribute for this type of user is:
  - ACEE association with SPECIALPGM records
- **Built in user** A user that is built in Privileged Access Manager. For example, `_undefined`.

#### NOTE

Only a Privileged Access Manager administrator can use this command.

This command has the following format:

```
secons -acee [handle | all | list]
```

- **all**  
Displays all ACEE records.
- **handle**  
Defines the ACEE handle you want to display.
- **list**  
Displays a summary list of all ACEE records, without the full details.

#### Examples: Display ACEE Records

- This example displays a list of handles in the ACEE:

```
secons -acee list
```

The `secons` output looks like this:

```
ACEE handle '0' represents 'Logged on User': NT AUTHORITY\ANONYMOUS LOGON (OS User)
ACEE handle '1' represents 'Logged on User': NT AUTHORITY\NETWORK SERVICE (OS User)
ACEE handle '2' represents 'Logged on User': COMPl-SRV-X86\John
ACEE handle '3' represents 'Logged on User': NT AUTHORITY\LOCAL SERVICE (OS User)
ACEE handle '4' represents 'Logged on User': NT AUTHORITY\SYSTEM (OS User)
ACEE handle '5' represents 'Management User': COMPl-SRV-X86\John
ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
```

- This example displays handle 6 in the ACEE:

```
secons -acee 6
```

The `secons` output looks like this:

```
ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
ACEE was created at: Wed Feb 20 17:35:52 2008
ACEE was last accessed at: Wed Feb 20 17:35:52 2008
ACEE user role is: Regular
ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User definition
ACEE user is a member of 0 'CA ControlMinder' groups
ACEE user is associated with 1 SPECIALPGM records
  1. C:\WINDOWS\system32\calc.exe
```

## secons -checkSID Function Resolve Recycled Accounts on Windows

### Valid on Windows

The secons utility compares the security identifier (SID) of each enterprise account (XUSER and XGROUP resource) with the native Windows account SID, and creates a backup of recycled accounts. As the Privileged Access Manager authorization is based on SID, where the SID of a Privileged Access Manager accessor resource differs from the native account SID (a recycled account), the utility creates a new account (with the same name as the old account) and backs up the obsolete resource using the following naming convention: *SID (accountName)*

#### NOTE

For more information on recycled enterprise store accounts, see the *Endpoint Administration Guide for Windows*.

This command has the following format:

```
secons -checkSID {-groups | -users} [accountName [,accountName...]]
```

- **-groups**  
Specifies that secons should examine enterprise group records.
- **-users**  
Specifies that secons should examine enterprise user records.
- **accountName**  
Specifies the name of a user or group that secons should search for. If *accountName* is omitted, secons looks for all groups or users.

## secons -i Function Display Run-time Statistics on Windows

### Valid on Windows

The secons utility displays Privileged Access Manager run-time statistics and internal counters. Use this statistical system behavior information to learn the following:

- How many events were triggered for each interception type.
- How effective each kernel cache is, by comparing the number of cached events against the number of fully authorized events.

**Note:** It is normal for the audit queue to increase in periods of increased activity. However, the queue size should decrease once the load is normal again.

This command has the following format:

```
secons -i [-reset]
```

- **-i**  
Displays runtime statistics as formatted text.
- **-reset**  
(Optional) Resets the run-time counters to zero.

### Example: Display run-time data

The following describes the information that is not self-explanatory in the output of the secons -i command:

- **Database run-time data**  
Displays the number of classes, objects, and properties in the Privileged Access Manager database, the ID of the last created class, object, and property, and the number of property values.

Use this information to evaluate the size of the database. The more objects and properties you use, the bigger the database is.

- **Kernel run-time data**

Displays for each of the kernel caches (file, registry, and surrogate) their creation time, size, and efficiency. Efficiency is the number of audit events out of the total number of events. The remaining interception events follow the authorization process.

Use this information to evaluate the need for, and efficiency of, each kernel cache.

- **Kernel audit information**

Displays the current kernel audit queue size and the maximum size it reached and when.

Use this information to evaluate the audit queue behavior. You should make sure that the audit queue does not exceed the maximum allocated queue size, which is set in the FsiDrv\MaxAuditRecordLimit Privileged Access Manager registry entry. When this limit is reached, Privileged Access Manager generates audit events more slowly so that the queue can be resolved.

- **User mode enforcement run-time data**

Displays information for intercepted file, registry, logon, kill, and Windows service events in Full Enforcement mode. You can find out about the number of events being authorized by the authorization engine and the maximum and average time an authorization process took to complete for each class.

Use this information to troubleshoot problems in a live production system. It provides you with some valuable initial data without needing to shut down Privileged Access Manager.

- **User mode audit run-time data**

Displays information for audit events (cached intercepted event).

Use this information to monitor user mode audit queue behavior. If the maximum audit queue increases consistently, make sure that Privileged Access Manager can write to the audit log file. Privileged Access Manager may not be able to write to the file if the system has run out of disk space, or it does not have native access permissions to file.

**Note:** It is normal for the audit queue to increase in periods of increased activity. However, the queue size should decrease once the load is normal again.

## secons -i Function Display Run-time Statistics on UNIX

### Valid on UNIX

The secons utility displays Privileged Access Manager run-time statistics about system behavior including:

Network connection requests.

- Current service levels for FILE protection rules
- The size of the audit and error log queues
- The size of cached tables
- The size of the database
- The number of records in each part of the database

This command has the following format:

```
secons -i
```

- **-i**  
Displays runtime statistics as formatted text.

### Example: Display run-time data

The following example shows the output of the secons -i command:

## Runtime Statistics:

-----

## INet statistics:

Requests denied : 0  
Requests granted : 17  
Errors found : 0

## Queues size:

Audit log: 0  
Error log: 0

## Cached tables info:

ACEE handles : 11  
Protected clients : 0  
Trusted programs : 77  
Untrusted programs: 3

## Database info: (Record count &amp; first free ID)

Classes : 235 ( CID 0x00f0 )  
Properties : 4829 ( PID 0x1346 )  
Objects : 842 ( OID 0x0000035a )  
PropVals : 4109 ( N/A )

## CA PAMSC memory utilization statistics:

-----

CA PAMSC security daemon (seosd, pid=4265 Total=13MB Res=8MB)

CA PAMSC agent daemon (seagent, pid=4268 Total=10MB Res=3MB)

CA PAMSC watchdog daemon (seoswd, pid=4276 Total=6MB Res=3MB)

CA PAMSC policyfetcher daemon (policyfetcher, pid=4331 Total=11MB Res=1MB)

CA PAMSC AgentManager daemon (AgentManager, pid=4561 Total=22MB Res=3MB)

Kernel load statistic:

```
Queue: ----- FILE: SEOS current queue depth : 0 SEOS max queue depth : 1 SEOS current queue rate
msec SEOS max queue rate : 0 req/
msec SURROGATE: SEOS current queue depth : 0 SEOS max queue depth : 1 SEOS current queue rate
msec SEOS max queue rate : 0 req/
msec Total: SEOS current queue depth : 0 SEOS max queue depth : 2 SEOS current queue rate : 0
msec SEOS max queue rate : 20 req/
msec Syscalls: ----- FILE: Active SEOS handlers : 0 syscs SEOS hanlers calling rate : 0.0866
msec(406 handlers within 4684 msecs) Average processing time : 0.014742 msecs (407 handlers wi
msec(363 handlers within 8368826 msecs) Average processing time : 0.126374 msecs (364 handlers
```

-----

The following code explains each line in the preceding output:

INet statistics:

```
Requests denied : 0
Requests granted : 17
Errors found : 0
```

Displays statistics of network access authorization that is performed by Privileged Access Manager. These lines summarize the number of denials, grants, and errors during the authorization of network requests.

Queues size:

```
Audit log: 0
Error log: 0
```

The product creates logging with file locking and so it is possible that certain events are held in memory and written to log files after a while. If these values exceed 10, then an error could be interfering with the product logging facility.

Cached tables info:

```
ACEE handles : 11
Protected clients : 0
Trusted programs : 77
```

Untrusted programs: 3

Displays information about the size of cached tables Privileged Access Manager uses:

- Accessor Element Entry (*ACEE*) is a table containing logged-in processes.
- *Protected clients* list the number of cached clients. Usually, this value is 0.
- *Trusted Programs* lists the number of entries in class PROGRAM that are cached in memory. Typically, all programs should be cached as trusted.
- *Untrusted Programs* displays the number of programs that were found to be untrusted.

Database info: (Record count & first free ID)

```
Classes      :    235 ( CID      0x00f0 )
Properties   :   4829 ( PID      0x1346 )
Objects      :    842 ( OID 0x0000035a )
PropVals     :   4109 ( N/A )
```

General information regarding the size of the database and the number of records in each part of the database.

Displays information about the size of the memory the following daemons use: seosd, seagent, seoswd, policyfetcher, and AgentManager:

CA PAMSC memory utilization statistics:

-----

CA PAMSC security daemon (seosd, pid=4265 Total=13MB Res=8MB)

CA PAMSC agent daemon (seagent, pid=4268 Total=10MB Res=3MB)

CA PAMSC watchdog daemon (seoswd, pid=4276 Total=6MB Res=3MB)

CA PAMSC policyfetcher daemon (policyfetcher, pid=4331 Total=11MB Res=1MB)

CA PAMSC AgentManager daemon (AgentManager, pid=4561 Total=22MB Res=3MB)

The Privileged Access Manager Watchdog daemon monitors the memory use of the daemons based on the interval that is defined in the ProcVSizeInterval token. If a process exceeds the specified watermark in the ProcVSizeHigh token, the Watchdog restarts the process within the time frame that is defined in the ProcRestartHours token. If a process exceeds the memory size that is specified in the ProcVSizeCritical token, the Watchdog daemon immediately restarts the process.

## secsn -kt Function Display Kernel Tables on UNIX

Valid on UNIX



The secons utility displays the kernel tables.

This command has the following format:

```
secons -kt tableNumber
```

- **-kt**  
Displays the specified kernel table.
- **tableNumber**  
Specifies the kernel table to display. *tableNumber* must be one of the following values:
  - **1**  
Specifies to display the SpecPgm kernel table.
  - **2**  
Specifies to display the TrustPg kernel table.
  - **3**  
Specifies to display the LoginPg kernel table.
  - **4**  
Specifies to display the DBfiles kernel table.
  - **5**  
Specifies to display the FRegExp kernel table.
  - **6**  
Specifies to display the DCMfile kernel table.
  - **7**  
Specifies to display the AC pids kernel table.
  - **8**  
Specifies to display the InoCach kernel table.  
**Note:** Not valid on Linux.
  - **9**  
Specifies to display the F cache kernel table.
  - **10**  
Specifies to display the NetwDCM kernel table.
  - **11**  
Specifies to display the MntDirs kernel table.
  - **12**  
Specifies to display the F inode kernel table.
  - **13**  
Specifies to display the STOPexp kernel table.  
**Note:** You cannot display this kernel table if STOP is not enabled.
  - **15**  
Specifies to display the Family kernel table.
  - **16**  
Specifies to display the DbgProt kernel table.
  - **17**  
Specifies to display the TCPport kernel table.
  - **18**  
Specifies to display the TCPoutp kernel table.
  - **19**  
Specifies to display the ProcSrv kernel table.
  - – **20**

- Specifies to display the ACEE kernel table.
- **21**  
Specifies to display the Status kernel table.  
**Note:** This option shows the status of all kernel tables.
- **22**  
Specifies to display the StreamSockets kernel table.  
**Note:** This option is for HP-UX and Solaris only when SEOS STREAMS module is enabled.
- **23** Specifies to display the KBLshell kernel table.
- **24** Specifies to display the KBLcmdlog kernel table.
- **25** Specifies to display the Devices kernel table.
- **26** Specifies to display the Auto bypassed programs kernel table.
- **27** Specifies to display the User cache kernel table.
- **all** Specifies to display all tables.

### Example: Display the DBfiles Kernel Table

**Note:** The following is an example of the output when you display the DBfiles kernel table:

```
secons -kt 4

DBfiles

file      ID  i-node  device  program name
-----
1    29  280391  356515  /opt/CA/PAMSC/seosdb/seos_ids.dat
2     3    0      0    /opt/CA/PAMSC/etc/privpgms.init
```

### Kernel Tables

Kernel tables list frequently-accessed information to help improve Privileged Access Manager performance. Kernel tables improve performance because Privileged Access Manager does not need to check the database to permit, deny, or resolve events that are listed in the kernel tables.

Privileged Access Manager includes the following types of kernel tables:

- **Cache tables** List the results of previous resource access requests, resolved inode numbers, and accepted incoming TCP requests.
- **Protected resource tables** List resources for which, when access is requested, Privileged Access Manager always sends an authorization request to the Privileged Access Manager engine.
- **Bypass tables** List resources for which, when access is requested, Privileged Access Manager permits access without sending an authorization request to the Privileged Access Manager engine.
- **Process table** Lists information about all the processes running in the system.

The following table provides information about each kernel table:

Table Name	Type	Lists	Column Names	Configuration Setting
SpecPgm	Protected resource	All objects in the SPECIALPGM class	flags; user; oid; i-node; device; program	SPECIALPGM class records
TrustPg	Protected resource	All objects in the PROGRAM class	flags; i-node; device; program	PROGRAM class records

LoginPg	Protected resource	All objects in the LOGINAPPL class	flags; i-node; device; program name	LOGINAPPL class records
DBfiles	Protected resource	All objects in the FILE class	file ID; i-node; device; program	FILE class records <b>Note:</b> The maximum number of records in this table is defined by max_regular_file_rules in the SEOS_syscall section of the seos.ini file
FRegExp	Protected resource	Generic file access rules that are defined in the FILE class	fid; expression	Defined by a generic rule in a FILE class record <b>Note:</b> The maximum number of records in this table is defined by max_general_file_rules in the SEOS_syscall section of the seos.ini file
DCMfile	Bypass	Do-not-call-me files that you define using GAC	fid; user; type; access	GAC.init file
ACpids	Bypass	Process IDs for the Privileged Access Manager daemons	pid; service; contractID	-
InoCach	Cache	Cached inodes	i-node; device; priority; entry	cache_enabled in the SEOS_syscall section of the seos.ini file
F cache	Cache	Cached file access authorization results	file ID; access; acee; answer; phash; prio	-
NetwDCM	Cache	Cached accepted incoming TCP connections	peer; port; local port; flag; prio	UseNetworkCache in the seosd section of the seos.ini file
MntDirs	Protected resource	Directories that Privileged Access Manager protects from mounting	dir ID; i-node; device; mount point	-
F inode	Protected resource	Inode and device number of objects in the FILE class	file ID; i-node; device; links	-
STOPbyp	Bypass	Objects in the PROGRAM class for which Privileged Access Manager does not provide STOP protection	i-node; device; program	If STOP is enabled, objects in this table have a SPECIALPGM record with the property pgmtype(STOP)
STOPexp	Bypass	Regular expressions that define objects in the PROGRAM class for which Privileged Access Manager does not provide STOP protection	priority; n-chars; expression	If STOP is enabled, objects in this table are defined by a generic rule in a SPECIALPGM record with the property pgmtype(STOP)
Family	Bypass	Privileged Access Manager daemons	service; pid; contractID	-

DbgProt	Protected resource	Privileged Access Manager binaries that Privileged Access Manager protects from debugging	pid; access; name in proc	-
TCPport	Bypass	Ports for which seos_syscall will not pass events to seosd	TCP port	bypass_TCPIP in the seosd section of the seos.ini file
TCPoutp	Bypass	Ports for which seos_syscall will not pass outgoing connection events to seosd	TCP port	bypass_outgoing_TCPIP in the seosd section of the seos.ini file
ProcServ	Process	Lists information about all the processes running in the system	#n; pid; ppid; acee; flags; uid; euid; zone; arg0; ACuser <b>Note:</b> There are many more internal columns in this table that are not displayed by the secons utility	-

### Kernel Table Column Names

The following list explains the kernel table column names:

- **#n**  
Entry number in the kernel table.
- **access**  
Defines the type of access that Privileged Access Manager permits, or the type of access that a user requested. The value is a sum of access types:  
**1-read2-write4-chown8-chmod16-rename32-unlink64-utimes128-chattr256-link512-chdir1024-create**
- **acee**  
Defines the ACEE of the user making the access request.
- **ACuser**  
Defines the Privileged Access Manager user name of the user.
- **answer**  
Defines the response (permit or deny) that Privileged Access Manager made to the access request. Valid values include:  
**0deny**  
**1permit**
- **arg0**  
Defines the program name, as defined in argument number 0 when the program executes.
- **contractID**  
(Solaris 10 only) Defines the contract process ID.
- **device**  
Defines the logical disk that the file resides on.
- **dir ID**  
Defines the directory ID.
- **entry**  
Defines the string value of the inode.
- **euid**

Defines the effective user ID.

- **expression**  
Defines the expression (text pattern used for string matching) that specifies the resources to which the entry applies.
- **fid or file ID**  
Defines the file ID that Privileged Access Manager uses to identify the file.
- **flags**  
Defines the bit mask flag for the entry.
- **i-node**  
Defines the inode number.
- **links**  
Defines the number of hard links of the file.
- **local port**  
Defines the port on the local host that accepts the incoming TCP connection.
- **mount point**  
Defines the location in the directory to protect from mounting.
- **n-chars**  
Defines the number of characters in the expression.
- **name in proc**  
Defines the process name in the /proc file system.  
**Note:** In the /proc file system, each process is represented as a file, and the file name is the process number.
- **oid**  
Defines the object ID.
- **peer**  
Defines the peer host address.
- **phash**  
Defines the hash value of a path string.
- **pid**  
Defines the process ID.
- **port**  
Defines the port from which the incoming TCP connection originated.
- **ppid**  
Defines the parent process ID.
- **prio or priority**  
Defines the priority of the entry in the kernel table. When the kernel table is full, the entry with the lowest priority is removed when Privileged Access Manager writes a new entry to the kernel table.
- **program or program name**  
Defines the name of the program.
- **service**  
Defines the name of the Privileged Access Manager service (daemon).
- **TCP port**  
Defines the TCP port to which the entry applies.
- **type**  
Defines the protected file type.
- **uid or user**  
Defines the user ID.
- **zone**  
(Solaris 10 only) Defines the zone ID.  
**Note:** The value of this column is always 0 for a non-Solaris 10 computer.

## Cache Tables

There are three types of kernel cache tables:

- **F cache** The file cache table caches the results of previous authorization requests. When an identical authorization request is made, Privileged Access Manager answers the request with the last response that is stored in the file cache table.

### NOTE

The file cache tables is cleaned every 30 minutes and whenever a record changes in the following classes: CALENDAR, CONTAINER, FILE, GFILE, GROUP, HOLIDAY, PROGRAM, SECLABEL, SECLEVEL, SHIFT, and USER.

- **InoCach** The inode cache table caches resolved inode numbers. When Privileged Access Manager needs to resolve an inode number to a file name, it checks the InoCach table before it checks the file system.
- **NetwDCM** The network cache table stores accepted, incoming TCP requests. When Privileged Access Manager receives an incoming TCP request that is identical to a request in the network cache, Privileged Access Manager automatically permits the request.

You can use the `secons` utility to display, clean, enable, and disable kernel cache tables.

## Protected Resource Tables

When Privileged Access Manager intercepts an authorization request, it checks if the resource to which access is requested is listed in the protected resource tables in the kernel.

If the resource is listed in the protected resource tables, Privileged Access Manager always sends an authorization request to the Privileged Access Manager engine. If the resource is not listed in the protected resource table, Privileged Access Manager may not send an authorization request to the engine but instead resolve the access request in the kernel.

## Bypass Tables

When Privileged Access Manager intercepts an authorization request, it checks if the resource to which access is requested is listed in the bypass tables in the kernel.

If the resource is listed in the bypass tables Privileged Access Manager permits the access request. If the resource is not listed in the bypass tables Privileged Access Manager passes the request to the Privileged Access Manager authorization engine for further access checks.

## secons -krc Function Clean, Enable, or Disable Kernel Cache Tables on UNIX

### Valid on UNIX

The `secons` utility cleans, enables, or disables the kernel cache tables.

This command has the following format:

```
secons -krc optionNumber
```

- **-krc**  
Specifies to clean, enable, or disable a kernel cache table.
- **optionNumber**  
Specifies the action to perform. *optionNumber* must be one of the following:
  - **1**  
Cleans the F cache table.
  - **2**

- Enables the F cache table.
- **3**  
Disables the F cache table.
- **4**  
Cleans the NetwDCM table.
- **5**  
Enables the NetwDCM table.
- **6**  
Disables the NetwDCM table.
- **7**  
Cleans the F inode table.

**NOTE**

Not valid on Linux.

- **8**  
Enables the F inode table.

**NOTE**

Not valid on Linux.

- **9**  
Disables the F inode table.

**NOTE**

Not valid on Linux.

**Example: Clean the F cache Table****NOTE**

The following example cleans the F cache table:

```
secons -krc 1
```

**secons -refIP Function Refresh IP Addresses for Network Resources****Valid on Windows**

The secons utility refreshes the IP addresses of database network resources. For the refresh to work on a particular host, the DNS must have already been refreshed on that host. Use the following Windows command to refresh the DNS manually:

```
ipconfig /flushdns
```

This command has the following format:

```
secons -refIP [hosts]
```

- **-refIP [hosts]**  
(Windows only) Defines a space-separated list of hosts on which Privileged Access Manager will refresh IP addresses for network resources. If no hosts are listed, local network resources are refreshed.  
This option lets you update Privileged Access Manager resources with the current IP address and is particularly useful in a DHCP environment where IP addresses are assigned dynamically.

**secons -rl Function Reload Configuration Settings and KBL on UNIX****Valid on UNIX**

The secons utility reloads the seos.ini file for seosd and the KBL (Keyboard Logger). This lets you update your configuration settings without having to shut down Privileged Access Manager.

This command has the following format:

```
secons -rl
```

- **-rl**  
(UNIX only) Reloads the seos.ini configuration file and updates settings without shutting down Privileged Access Manager.

## secons -v Function Control Instrumentation Run-time Settings on Windows

### Valid on Windows

The secons utility controls Privileged Access Manager instrumentation run-time settings. You can use the utility to load an external DLL library into an active process and modify the run-time tracing configuration of Privileged Access Manager instrumentation plug-ins. You must have the ADMIN or OPERATOR attribute to execute this command.

This command has the following format to load a DLL library:

```
secons -v target load "dll_name"
```

This command has the following format to enable or disable the trace on a Privileged Access Manager instrumentation plug-in:

```
secons -v target trace plugin_name {trace:enable|trace:disable}:{file:"tracefile_path"|debug}
```

### NOTE

Privileged Access Manager does not start the trace until the trace is correctly configured.

This command has the following format to configure the trace on a Privileged Access Manager instrumentation plug-in:

```
secons -v target trace plugin_name trace:option:{sources:{1 | 4} | filtering:value | filecyclic:{0 | 1} | filelimit:value }
```

- **debug**  
Specifies that the command enables or disables tracing to the debug output channel.
- **file:"tracefile\_path"**  
Defines the full path to the file that Privileged Access Manager writes the trace to.

### NOTE

If you specify the trace:disable parameter, Privileged Access Manager ignores any value that you specify for the file:"tracefile\_path" parameter.

- **filecyclic:{0 | 1}**  
Specifies if cyclic file tracing is enabled. If you enable cyclic file tracing, when the size of the trace file reaches the specified maximum size, Privileged Access Manager returns to the start of the trace file and continues writing the trace.  
This parameter has the following values:  
**0**-Disable cyclic file tracing  
**1**-Enable cyclic file tracing
- **filelimit:value**  
Defines the maximum size, in bytes, of the trace file. A value of 0 means the trace file has no maximum size.
- **filtering:value**  
Defines the bitwise filter mask that filters the trace for the specified instrumentation plug-in. Privileged Access Manager does not write filtered events to the trace file.



**NOTE**

To specify no filtering, that is, to specify that Privileged Access Manager writes all events to the trace, use the following value: 0xFFFFFFFF. All other values for this parameter depend on the plug-in that you specify.

- **load "*dll\_name*"**  
Specifies to load the specified DLL into the target process. The DLL operating environment and the target process operating environment must be identical. For example, if you specify a 32-bit process as the target process, the DLL must also be 32-bit.

**WARNING**

The DLL must be located in the *ACInstallDir\bin* folder.

- **sources:{1 | 4}**  
Specifies where Privileged Access Manager outputs the trace.  
This parameter has the following values:  
**1**-Output to file  
**4**-Output to debug API trace
- **target**  
Defines the target process or processes. This parameter has one of the following values:
  - **all\_32bit**  
Specifies to send the command to all 32-bit processes running on the computer.
  - **all\_64bit**  
Specifies to send the command to all 64-bit processes running on the computer.
  - **PID**  
Defines the process ID of the target process. The target process must be running on the computer.
  - **process\_name**  
Defines a mask that identifies the names of the target process. The target process must be running on the computer. For example, if you specify cmd.exe for this parameter and there are three instances of cmd.exe running on the computer, Privileged Access Manager applies the command to all three processes.
- **trace *plugin\_name***  
Specifies to modify the run-time tracing configuration for the Privileged Access Manager instrumentation plug-in named *module\_name*, for example, cainstrm or stopplg.

**NOTE**

You must specify the DLL name of the plug-in. If you upgrade an instrumentation plug-in and the name of the DLL for the plug-in changes, you must specify the name of the new DLL in the command. For example, if you upgrade the cainstrm plug-in and the name of the upgraded DLL for the plug-in is cainstrm2.dll, you must specify cainstrm2 as *plugin\_name*.

- **trace:disable**  
Specifies to enable the trace on the target plug-in.
- **trace:enable**  
Specifies to disable the trace on the target plug-in.

**NOTE**

This parameter changes the status of the trace enabled flag in run time. Privileged Access Manager does not begin the trace until the trace is correctly configured.

- **trace:option**  
Specifies to configure the trace on the target plug-in.

**Example: Enable Tracing to the Debug Output Channel**

The following command changes the status of the trace enabled flag in run time for all files in the stopplg plug-in that are in 32-bit processes running on the computer. Privileged Access Manager does not begin the trace until the trace is correctly configured:

```
secons -v all_32bit trace stopplg trace:enable:debug
```

### Example: Apply a Trace Filtering Mask to a Plug-in

The following command applies a trace filtering mask to all files in the cainstrm plug-in that are in the process with PID 362:

```
secons -v 362 trace "cainstrm trace:option:filtering:4294967295"
```

### secons -whoami Function Display Your User Name and Security Credentials

#### Valid on Windows

The secons utility displays the user name as it is known to the Privileged Access Manager authorization engine. This is the information that it stores in the Accessor Element Entry (ACEE) table. The ACEE stores information about the following users:

- **Logged in user**A user that has logged in to the operating system. Specific ACEE attributes for this type of user are:
  - Login session ID
  - Login session type
- **Management user**A user that has logged in to a Privileged Access Manager management application (using an LCA connection). For example, selang.
- **Authorization API user**A user that was referenced in SEOSROUTE\_\* API.
- **SPECIALPGM Logical user**A user that is being references at least in one SPECIALPGM record. A specific ACEE attribute for this type of user is:
  - ACEE association with SPECIALPGM records
- **Built in user**A user that is built in Privileged Access Manager. For example, *\_undefined*.

This command has the following format:

```
secons -whoami
```

### Example: Display Your User Name and Security Credentials

This example displays your own user name and security credentials as they are known to the Privileged Access Manager authorization engine:

```
secons -whoami
```

The secons output looks like this:

```
ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86\John
```

```
ACEE was created at: Wed Feb 20 17:34:47 2008
```

```
ACEE was last accessed at: Wed Feb 20 17:36:49 2008
```

```
ACEE user role is: Auditor, Administrator
```

```
ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User definition
```

```
ACEE user is a member of 0 'CA PAMSC' groups
```

ACEE's Logon session ID is: 0:68737

ACEE's Logon session type is: Interactive

## secons Manage Enabled Kernel

This command has the following format:

```
secons [-dk] [-ek] [-ik]
```

- **-dk**  
Disable kernel extension

### WARNING

Use this parameter only when instructed to do so by CA Support.

- **-ek** <kernel extension name>  
Enable kernel extension
- **-ik**  
List kernel extensions

## secons -raf Function Reloads the audit.cfg file and KBL

### Valid on UNIX

The secons utility reloads the audit.cfg file for seosd and KBL (Keyboard Logger), and also reloads the auditrouteft.cfg file for ReportAgent.

This command has the following format:

```
secons -raf
```

- **-raf**  
(UNIX only) Reloads the the audit.cfg file for seosd and KBL (Keyboard Logger), and also reloads the auditrouteft.cfg file for ReportAgent. It updates the configuration settings without shutting down Privileged Access Manager.

## secrepsw Utility Create Policy Model and Shadow Files

### Valid on UNIX

The secrepsw utility creates a password record for every user in the /etc/passwd file. This is necessary for administering users defined by PMDBs operating over a UNIX environment. The utility can also create and remove shadow files.

### NOTE

This utility is located in the lbin directory and only root can use it. You must change the shadow token in the pmd.ini file to yes before you use this utility.

This command has the following format:

```
secrepsw [-h] [-c] [-r PolicyModel] [-s PolicyModel]
```

- **-c**

Creates a new Policy Model password file from the /etc/passwd and /etc/shadow files on the local computer.

- **-h**  
Displays the help for this utility.
- **-r *PolicyModel***  
Transfers user names and passwords from the Policy Model's shadow file back to the original Policy Model password file (passwd).
- **-s *PolicyModel***  
Transfers user names and passwords from the Policy Model password file (passwd) to the Policy Model's shadow file.

## sedbpchk Utility Back Up the Database

### Valid on UNIX

The sedbpchk utility creates a backup copy of the database. It copies the runtime database to a temporary location, performs various database integrity checks on the temporary database, and, if the database passes the checks, copies the temporary database into a backup location.

If the database does not pass the integrity tests, sedbpchk tries to determine whether any updates were applied to the database while the copy was being made. If there were updates, the conclusion that the database is corrupted may not be accurate.

If there were no updates while the database was being copied, the conclusion that the database is corrupted is probably true. In that case, a mail message is sent to the system administrator, who can then use the backup directory to override the corrupted runtime database.

### NOTE

This script is *not* foolproof. It may conclude that a database is corrupted when it is not. However, the conclusion that a database is okay is always accurate.

You must have root and ADMIN privileges to run this script. Before using sedbpchk, we recommend that you review the script, located in *ACInstallDir/bin* as sedbpchk.sh, to confirm that the values of the following fields match the needs of your site.

- **MAIL\_TO**  
Specifies the name of the user who is sent the notification that the database is corrupt.
- **RETRIES**  
Specifies the number of times the utility checks the database when it suspects that the database is corrupted before sending the notification.
- **ACInstallDir**  
Specifies the location of the Privileged Access Manager installation directory.
- **SE\_BINDIR**  
Specifies the location of the Privileged Access Manager binary files directory.
- **SE\_DB\_DIR**  
Specifies the location of the Privileged Access Manager runtime database directory.
- **SE\_BCKDIR**  
Specifies the location of the backup database directory.
- **SE\_TMPDIR**  
Specifies the location of the temporary database directory.

### NOTE

This utility is supplied as a script file; you need to specify the .sh extension to run it.

This command has the following format:

```
sedbpchk
```

## seerrlog Utility Display Error Log Records

### Valid on UNIX

The seerrlog utility displays the records in the Privileged Access Manager error log. You must either have permission to read the error log file, or be a member of the group that can read the error log files (the group defined in the configuration setting `error_group`).

This command has the following format:

```
seerrlog [-h] [-s date] [-e date] [-d] [-f filename]
```

- **-s date**  
Specifies the start date for the list. Lists records written on and after the defined date.  
**Limits:** Date should be in the format dd-mm-yyyy.
- **-e date**  
Specifies the end date for the list. Lists records written up to and including the defined date.  
**Limits:** Date should be in the format dd-mm-yyyy.
- **-d**  
Specifies *not* to print the detailed information of failures.
- **-h**  
Displays the help for this utility.
- **-f filename**  
Specifies the error log file to read.  
By default, seerrlog reads the `ACInstallDir/log/seos.error` file. You cannot define this file in the database, and only Privileged Access Manager can write to the file.

### Examples

- To list all error records written since 3 January 2006, specify:  

```
seerrlog -s 03-Jan-2006
```
- To list all error records written between 3 January 2006 and 1 January 2007, specify:  

```
seerrlog -s 03-Jan-2006 -e 01-Jan-2007
```

## segrace Utility Display User Login Information

The segrace command line utility displays the number of grace logins left for a user, the number of days remaining until the user's existing password expires, or the date and time the user last logged on, and from which terminal.

### NOTE

For more information about the grace login property of a user, see the *Endpoint Administration Guide* for your OS.

Before segrace can work, the system administrator must activate Privileged Access Manager password checking by entering the selang command:

```
setoptions class+(PASSWORD)
```

Subsequently, every time a user's password is changed, the new password is checked against the password quality rule set in the database.

## segrace Utility Display User Login Settings on UNIX

### Valid on UNIX

The `segrace` utility displays login settings for a user. We recommend that you run the `segrace` command every time a user logs in. To do so, add the command to `/etc/profile` and `/etc/csh.login` (or `/etc/.login` for Solaris).

To permit `segrace` to count grace logins, you must use the `sepass` utility to change passwords. If users have no grace logins left, `segrace` invokes the `sepass` utility, which requests that the users replace their passwords. Your site may decide which command to execute instead of the `sepass` utility by specifying another utility in the `sepass_command` token in the `segrace` section of the `seos.ini` file.

This command has the following format:

```
segrace [-h] [-d days] [-l] [-p] [userName]
```

- **-d *days***  
Displays the number of days that remain until the user's current password expires. The number appears only if the number of days you specify in the *days* parameter is greater than, or equal to, the interval value in the Privileged Access Manager option. If you omit the *days* parameter, `segrace` uses a default of seven days. This option works only if the user's password was changed using `sepass`.
- **-h**  
Displays the help for this utility.
- **-l**  
Displays the date and time the user last logged in, and from which terminal.
- **-p**  
Prompts for a new password when a user's password has expired.
- ***userName***  
If you specify a user name, and the requester has the ADMIN attribute, `segrace` displays the required login information for the specified user.  
If you do not specify a user name, `segrace` displays the login details for the current user.

## segrace Utility Display User Login Settings on Windows

### Valid on Windows

The `segrace` utility displays login settings for a user. This utility can be executed from a remote machine, as a standalone module.

#### NOTE

If you invoke `segrace` without any parameters, and no grace logins are found for a user, `segrace` does not display anything.

This command has the following format:

```
segrace [-h] [-d days] [-l] [-p] [-s host] [userName]
```

- **-d *days***  
Sets the warning *days* parameter to be different from the default one configured in the server.
- **-h**  
Displays the help for this utility.
- **-l**  
Displays the date and time the user last logged in, and from which terminal.
- **-p**  
Prompts for a password warning if the password is about to be expired in the *warning days* period and/or if the user has a grace count.
- **-s *host***  
Specifies the remote server name where the Privileged Access Manager database will be used.
- ***userName***

If you specify a user name, and have the ADMIN attribute, segrace displays the required data for the specified user.  
If you do not specify a user name, segrace displays the login details for the current user.

## SegraceW Utility Check Password Expiry on Windows

### Valid on Windows

This Windows GUI grace utility checks whether the user's password has expired and/or the user has a grace login count. If it has, SegraceW displays a window in which the user can replace the password.

SegraceW can be executed as a standalone module in a non-Privileged Access Manager environment. This enables you to apply this utility on any workstation in a domain.

SegraceW tries to connect first to the primary domain controller (in an NT 4.0 environment). SegraceW looks for backup domain controllers only if the attempted connection fails. In a Windows 2000 or later environment, SegraceW tries to connect to the first domain controller it finds.

#### NOTE

If a remote host is specified explicitly in the SegraceW execution options, then SegraceW connects only to the remote host.

The SegraceW utility is designed to be called from login batch files located at Domain Controller's NETLOGON share.

The SegraceW utility checks whether the user password has expired and/or the user has a grace login count.

#### NOTE

For segraceW implementation in a domain environment, you must install MS VC++ 2005 Redistributable to the member server. The installation must be equivalent to the Privileged Access Manager installation on the remote server.

If the grace login count attribute of the user exists, then:

- If the number of remaining grace logins for the user is zero, SegraceW forces the user to change the password.
- If the number of remaining grace logins for the user is positive, SegraceW advises the user to change the password.

If the user does not have a grace login count, SegraceW checks password expiration status.

- If the password is about to be expired in a time frame larger than the value of the *warning days* parameter configured at the server side, SegraceW does nothing.
- If the password is about to expire in a time frame equal or less than the value of the *warning days* parameter configured at the server side, SegraceW advises the user to change the password.
- If the password has been expired, SegraceW forces the user to change the password.

When changing the password, SegraceW displays a change password message that asks the user to provide the old password, the new password, and confirm the new password.

After passing confirmation check, the password is updated in the domain controller's SAM database.

This command has the following format:

```
segracew [d] [-s host]
```

- **d**  
Sets the *warning days* parameter to be different from the default configured in the server.
- **-s host**  
Connects to the specified remote or local host to retrieve information.

#### NOTE

Before you can connect to a remote host, copy the encryption library from the remote host to the local host and rename it to defence.dll.

## seini Utility Manage Configuration Files

### Contents

#### Valid on UNIX

The `seini` utility manages Privileged Access Manager database and initialization files for any host. For any host, the `seini` utility can do the following:

- Display the path of the Privileged Access Manager database
- Display the path of an initialization (.ini) file
- Display the contents of a token from an initialization file
- Set the value of a specific token in a specific section of an initialization file
- Delete a specific token from a specific section of an initialization file

The `seini` utility also displays all tokens in any of the other .ini files. The name of the initialization file must always end in the suffix `.ini`. You can work on an .ini file from any remote host as long as you have `WRITE` and `ADMIN` privileges.

If you do not specify any switch, `seini` displays the paths of the database and the `seos.ini` file.

#### NOTE

The `seini` utility can only update the `seos.ini` file when `seosd` is *not* running, or when a rule in the database specifically permits it.

`seini` can perform an intelligent token and section search, by including certain tokens in the `seos.ini` file. This feature checks for spelling errors by comparing each token or section with the one you specified until it finds an exact or partial match (within a 25% error margin). If it finds the relevant token or section, `seini` performs the specified operation; otherwise it displays an error message.

#### NOTE

The intelligent search feature works only on the host where you invoke the `seini` utility.

This command has the following format:

```
seini [-d] [host]
seini [-i] [host]
seini [-H host] \
{[-f [host.]section.token [ini_file]] | \
[-r [host.]section.token [ini_file]] | \
[-s [host.]section.tokenvalue [ini_file]] | \
[-sn [host.]section.tokenvalue [ini_file]] }
```

- **-d [host]**  
Displays the path of the database on the remote host. If you do not specify a host, `seini` displays the path of the local host.
- **-f [host.]section.token [ini\_file]**  
Displays the value of the token in the section of the specified initialization file on a specified host. If `seini` cannot find the specified section or token, an empty line appears. You must separate the host, section, and token names with a period (.). If you do not specify the *ini\_file*, Privileged Access Manager searches the `seos.ini` file for the section and token. To display information about the local machine, omit the *host* parameter.
- **-g section**  
Displays a list of tokens in the defined section.
- **-h**  
Displays the help for this utility.
- **-H [host]**  
Specifies the remote host to be used with the `-f`, `-r`, `-s`, and `-sn` flags.
- **-i [host]**



Displays the pathname of the initialization file seos.ini. If you do not specify a host, seini displays the pathname on the local host.

- **-r [host.]section.token [ini\_file]**  
Deletes the token from the section of the initialization file in the specified host. If you do not specify the *ini\_file*, Privileged Access Manager deletes the token from the seos.ini file.  
To delete information on the local machine, specify the section and token names only.
- **-s [host.]section.token value [ini\_file]**  
Sets the value of the token in the section of the initialization file in the specified host. If you do not specify the *ini\_file* parameter, Privileged Access Manager sets the value in the seos.ini file. If the section or token does not exist, and you specified a remote host, Privileged Access Manager creates that section or token.  
To create a section or token on the local machine, use the -sn switch.
- **-sn [host.]section.token newValue [ini\_file]**  
Sets the value of the token in the section of the initialization file in the specified host. If you do not specify the *ini\_file* parameter, Privileged Access Manager sets the value in the seos.ini file. If the section or token does not exist, and you specified the local host, Privileged Access Manager creates that section or token.  
To create a section or token on a remote machine, use the -s switch.

### Examples: Using seini

- To find out where the seos.ini initialization file is located on the local computer, use the following command:  

```
seini -i
```
- To find out the value of the *trace* configuration setting in the [seosd] section, use the following command:  

```
seini -f seosd.trace_file
```
- To set the value of the *trace\_to* configuration setting in the [seosd] section, use the following command:  

```
seini -s seosd.trace_to file
```

The command output should look like this:

```
The token seosd.trace_to now set to file (was file,stop)
```

### selang Utility Run the Privileged Access Manager Command Line

The selang utility invokes a command shell that provides access to the Privileged Access Manager database and the native environment. The database is updated dynamically by issuing selang commands from within the command shell.

#### NOTE

The result of the command's execution is sent to the standard output unless you include the -o option.

This command has the following format on UNIX:

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] \
[-u userpass]
selang [-l] [-o file] [-r file] [-s] [-u userpass]
```

This command has the following format on Windows:

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] [-v]
selang [-l] [-o file] [-r file] [-s] [-v]
```

- **-c command**  
Specifies the selang command to execute. After selang executes the command, it exits.  
If *command* contains any spaces, enclose the entire string in quotation marks. For example:  

```
selang -c "showusr rosa"
```
- **-d path**  
Specifies that selang commands update the database in the defined path.  
**Note:** You can only specify a local database.
- **-f file**  
Specifies that selang commands are read from the defined file rather than from the terminal's standard input.

As `selang` executes the commands in the input file, the line number of command being executed appears on the screen. The `selang` prompt does not appear on the screen. After `selang` executes the commands in *file*, it exits.

- **-h**  
Displays the help for this utility.
- **-l**  
Specifies that `selang` updates the default local database, usually `ACInstallDir/seosdb` (where `ACInstallDir` is the directory where you installed Privileged Access Manager).  
You do not need to specify this option with `-d` or `-p`.

**NOTE**

This option replaces `selang`. It is only valid when `seosd` is not running, and only an Privileged Access Manager administrator with sufficient native privileges to update the database files can execute it.

- **-o file**  
Specifies that `selang` output is written in the specified file. Each time you invoke `selang`, it creates a new, empty file. If you specify the name of an existing file, `selang` writes over the information currently in the file.
- **-p pmdb**  
Specifies that `selang` commands update the database of the defined PMDB, which must be in the local station (this is the database in the PMDB subdirectory). Changes to the database are not propagated to subscribers.

**NOTE**

This option is not valid if either `sepmdd` or `seosd` is running on the specified PMDB and is not the same as using the *hosts command*.

**WARNING**

Do not make changes that require propagation in this mode. If you use native mode when making updates, Privileged Access Manager updates only the native host files (as defined in the Privileged Access Manager configuration options).

- **-r file**  
Specifies that `selang` reads the commands from the defined file. The file should consist of commands in normal `selang` syntax, separated by semicolons or line breaks. After executing the commands in *file*, `selang` prompts the user for input.  
If you do not define a file for this option, `selang` uses the `.selangrc` file in your home directory.
- **-s**  
Specifies that `selang` opens in silent mode, without displaying the copyright message.
- **-u user pass**  
(UNIX only) Specifies a username and password for running `selang`.  
To use this option, you must set the `check_password` token in the `seos.ini` file to `yes`; this causes Privileged Access Manager to prompt you with Enter your password when you run `selang -u`. You have three attempts to login.  
The token `no_check_password_users` in the `[lang]` section of the `seos.ini` file contains a list of users that bypass the password checking during a login to `selang`.

**NOTE**

If the `check_password` token is set to `no` (the default), `selang` does not require any passwords.

- **-v**  
(Windows only) Writes command line to output.

Usage notes:

- If `-h` is used, all other options are ignored.
- You cannot use the `-c` option with the `-f` option.
- You cannot use the `-d` option with the `-p` option.
- If you specify `-d` or `-p`, you do not need to specify `-l`.

## seldapcred Utility Encrypt and Store a Credential

### Valid on UNIX

The seldapcred utility encrypts and stores a credential you provide. This credential is used by LDAP-enabled Privileged Access Manager utilities (such as sebuildla) for retrieving data from an LDAP Directory Information Tree (DIT). Together with the value of the ldap\_userdn token in the [seos] section of the seos.ini file, it lets the utility authenticate to the LDAP service. For a simple authentication, the credential is a password corresponding to the ldap\_userdn value. For SASL authentication, the credential has different semantics.

The seldapcred utility writes the encrypted credential to *ACInstallDir/etc/ldapcred.dat*

This command has the following format:

```
seldapcred [-h] [-w [credential]]
```

- **-h**  
Displays the help for this utility.
- **-w [credential]**  
Specifies the credential you want seldapcred to encrypt and store. If you do not provide input to the seldapcred utility, it prompts you to enter this value. By using the interactive mode in this way, you prevent exposing the credential to other users.

## seload Utility Load and Start CA Privileged Access Manager Server Control

### Valid on UNIX

The seload utility loads the Privileged Access Manager extension to the UNIX kernel and starts the Privileged Access Manager daemons. The seload utility loads Privileged Access Manager daemons locally and remotely. It also determines whether the Privileged Access Manager extension to the UNIX kernel is loaded on the specified host. If seosd is not running, seload starts the daemon on the specified host. If you omit the -r switch and parameter, the seosd daemon runs on the local host.

You can instruct seload to load one of the following daemons on the remote host: seosd, selogrd, selogrcd, or serevu. This process depends on the tokens.

Use seload if Privileged Access Manager is placed in the boot sequence of the server station.

### NOTE

- When Privileged Access Manager is installed, sample initialization files for every operating system supported by Privileged Access Manager are placed in the *ACInstallDir/samples/system.init* directory. Use these files if Privileged Access Manager is to be started as part of the system initialization.
- The seload utility requires that the executable se\_loadtest be located in *ACInstallDir/sbin* (where *ACInstallDir* is the installation directory). This program determines whether the Privileged Access Manager extension to the UNIX kernel is loaded.
- When working remotely, the seload utility requires the following:
  - The executable rseload is located in Privileged Access Manager dir/sbin. This program runs on the remote host and activates seload.
  - The file /etc/services contains seosload service. You should add this file during Privileged Access Manager installation.
  - The file /etc/inetd.conf contains the rseload program. You can add this program during Privileged Access Manager installation.

This command has the following format:

```
seload [-c] [-nopmd] [-r host [daemon]]
```

- **-c**  
Changes the encryption key that was set using the `sechkey -r` command.
- **-nopmd**  
If you specify the `-c` switch with the `-nopmd` switch, `seload` does not update the Policy Model update file with the new key.
- **-r *host [daemon]***  
Loads the `seosd` daemons, and any other daemon specified in the `[daemons]` section of the `seos.ini` file.  
If you specify a *daemon*, `seload` starts only that daemon; it ignores the `seos.ini` token. You must supply with the daemon's full path.  
The `seos.ini` token in the `[daemons]` section is used only if you specify a value. It has no default value. If you do specify a value, `seload` substitutes the value in the token for the standard values of the specified utility or program. For example, if you specify the value `selogrd=yes`, `seload` automatically starts the `selogrd` daemon after it starts the `seosd` daemon.

## selogmix Utility Split and Merge Audit Log Files

### Valid on UNIX

The `selogmix` utility splits and merges Privileged Access Manager audit log files.

This command has the following format:

```
selogmix {-s|-m} [-fn fileName] [-l fileName1fileName2] \
[-c weight1:weight2] [-t days] [-d] [-i]
```

- **-c *weight1:weight2***  
Specifies the correlation of file sizes for splitting files where *weight1* indicates the relative weight of the first file and *weight2* indicates the relative weight of the second file. If you omit this option, `selogmix` uses a one-to-one correlation.
- **-d**  
Specifies to run `selogmix` in debug mode. In this mode, `selogmix` displays all settings.
- **-fn *fileName***  
Specifies the name of the audit log file to be split or the resulting file of a merge. If you omit this option, `selogmix` uses the file name specified by the `audit_log` token in the `[logmgr]` section of the `seos.ini` file.
- **-h**  
Displays the help for this utility.
- **-i**  
Specifies to run `selogmix` in interactive mode. In this mode, `selogmix` prompts you for confirmation before overwriting existing files; otherwise, it overwrites without confirmation.
- **-l *fileName1 fileName2***  
Specifies the files used in the merge or split operation.  
You must specify both file names for this option. For merging, specify the two file names you want to merge; for splitting, specify the two destination files. If you omit this option, `selogmix` uses the file name specified by the `audit_log` token in the `seos.ini` file and suffixes 1 and 2 to the file name.
- **-m**  
Merges two audit log files.
- **-s**  
Splits a specified audit log file.
- **-t *days***  
Specifies a number of days. You can only use this option for splitting files. Specify how many days from the end of logging to put into a separate file. If you omit this option, `selogmix` separates one last logging day.

### Examples

- To split the standard log file into two files of equal size, use the following command:

```
selogmix -s
```

The original audit file is named *ACInstallDir/log/seos.audit*

The new split files are named *ACInstallDir/log/seos.audit1* and *ACInstallDir/log/seos.audit2*.

- To separate records for the last two days from the log file, use the following command:

```
selogmix -s -t 2
```

- To split a log file into two files with a defined correlation in size, use the following command:

```
selogmix -s -c 1:2
```

- To merge two specified files into one named file, use the following command:

```
selogmix -m -l seos.audit1 seos.audit2 -fn seos.audit.merge
```

## semsgtool Utility Maintain the Message File

The semsgtool utility lets you:

- Show a single message from the Privileged Access Manager message file
- List an entire section of messages
- Dump the entire file into ASCII files, one ASCII file for each section
- Build a new message file
- Change message to a new one
- List messages, including substring
- Validate the message file

You can only specify one command each time you execute semsgtool.

The default location of the message file is *ACInstallDir/data/seos.msg*

### NOTE

The Privileged Access Manager message file is comprised of sections and message numbers. Each section holds messages for different Privileged Access Manager modules or sub-modules.

This command has the following format:

```
semsgtool {-build|-b} asciiSourceFileOutputMessageFile
semsgtool {-change|-c} [messageFile] {0xerror-code|section#msg#}new-message
semsgtool {-dump|-d} messageFile
semsgtool {-list|-l} [messageFile] sectionNumber
semsgtool {-number|-n} [messageFile] subString
semsgtool {-show|-s} [messageFile] [0xerror-code|section#msg#]
semsgtool {-validate|-v} [messageFile]
```

- **-build|-b**  
Creates a new Privileged Access Manager message file from an ASCII source file.
- **-number|-n**  
Lists messages in the message file that include a defined string.
- **-change|-c**  
Creates a new message file, named *messageFile.new*, where the specified message has the defined modified string.
- **-dump|-d**  
Dumps the message file into several files, one file for each section of the message file. This creates ASCII source files that later can be used to create new Privileged Access Manager message files.
- **-h**  
Displays the help for this utility.
- **-list|-l**

Lists all the messages in a given section in the message file.

- **-show|-s**  
Shows the message associated with a specific message code.
- **-validate|-v**  
(Windows only). Validates the message file by checking for duplicate messages and messages that exceed the allocated boundaries.
- **0xerror-code**  
Defines the hex number of the error code for the message that you want to display or change.
- **asciiSourceFile**  
Defines the source file in ASCII format from which semsgtool builds a new message file.
- **messageFile**  
Defines the name of the message file. If you omit this option, semsgtool uses the message file as specified in the configuration settings.
- **OutputMessageFile**  
Defines the name of a new message file to build.
- **section# msg#**  
Defines the section number and message number of the error code for the message that you want to display or change.
- **sectionNumber**  
Defines the section number of the section you want to list all the messages for.

### Example

- To list the message associated with the error code 0x205, enter the following command:  

```
semsgtool -s seos.msg 0x205
```
- To list the messages in section 512, enter the following command:  

```
semsgtool -l seos.msg 512
```
- To create a modified Privileged Access Manager message file, follow these steps:
  - a. Create a new message file with a modified message:  

```
semsgtool -c 0x2501 "This is the new message"
```

  
A new message file, seos.msg.new, is created with the modified message.
  - b. Copy the new file over the Privileged Access Manager message file:  

```
copy seos.msg.new seos.msg
```

  
Copies the new message file with the modified message on top of the old seos.msg file.
- To show the message associated with the error code 0x0205, enter the following command:  

```
semsgtool -s 0x205
```

## senable Utility Enable a Disabled User Account

### Valid on UNIX

The senable utility enables the login of a user that was disabled for any reason, at any location at which the user was disabled, including PMDBs. For example, the serevu daemon might disable a user, or the user's suspend date or expire date arrived.

After the senable utility enables the user account, it calls the sepass utility, which prompts for a new user password. To restore the most recent password, use the -n option.

The senable utility enables an undefined user account by deleting that account from the local /etc/passwd file.

To execute senable remotely, specify your local terminal needs in a rule that grants it WRITE permission for accessing the remote station. Otherwise, you cannot perform Privileged Access Manager administration there.

**NOTE**

For more information about remote administration restrictions, see the section [Endpoint Administration for UNIX](#).

This command has the following format:

```
senable [-host hostname] userNames [-n]
```

- **-host *hostname***  
Selects the host with the account to change from disabled to enabled.  
You must have ADMIN or PWMANAGER attributes on two hosts to use the -host option:
  - The host with the account to be changed from disabled to enabled.
  - The host where you enter the senable command.
- **-h**  
Displays the help for this utility.
- **-n**  
Runs the command noninteractively. If you use this option, senable does not call sepass, and restores the most recently used password.
- ***userNames***  
Defines a space-separated list of user names for accounts being changed from disabled to enabled.

## senone Utility Execute a Command as an Unauthorized User

### Valid on UNIX

The senone utility executes a command issued by a highly authorized user as an unauthorized user process.

**NOTE**

Only highly authorized users who are testing untrusted programs should use this utility.

When you invoke the senone utility, it deletes the process credentials from the authorization daemon. senone then executes a shell with the credentials of a user who is not defined to Privileged Access Manager. From this point on, any program invoked from within this shell is executed with the credentials of the non-Privileged Access Manager user. Because senone does not change the invoker's user ID, the user's UNIX privileges remain unchanged.

**WARNING**

We recommend that users who are logged in as root not run untrusted programs. Even when running untrusted programs with senone, unexpected problems can occur.

If you invoke senone without specifying a command, it executes the user's shell as defined in /etc/passwd.

This command has the following format:

```
senone [command]
```

- **-h**  
Displays the help for this utility.
- ***command***  
Specifies the command you want senone to execute as an unauthorized user.

## SEOS\_load Utility Load the CA Privileged Access Manager Server Control Interception Module

### Valid on UNIX

The SEOS\_load utility controls the dynamic Privileged Access Manager kernel module (SEOS\_syscall). The interception module must be loaded before running any Privileged Access Manager utility.

**NOTE**

You can use UNIX exits to automatically run programs before and after loading and unloading the kernel.

On streams supported platforms, this utility loads the Privileged Access Manager module to streams depending on the SEOS\_use\_streams token in the [SEOS\_syscall] section of the seos.ini file. If the token is set to yes, the module is pushed into streams.

This command has the following format:

```
SEOS_load [-i|-k|-s|-u]
```

- **-i**  
(For HP-UX and Sun Solaris platforms only.) Displays information about the Privileged Access Manager kernel extension.
- **-k**  
(For HP-UX and Sun Solaris platforms only.) Loads the Privileged Access Manager module into the kernel without pushing into streams.
- **-s**  
(For HP-UX and Sun Solaris platforms only.) Inserts the Privileged Access Manager kernel module into streams. This option ignores the SEOS\_use\_streams token in the SEOS\_syscall section of the seos.ini file.
- **-u**  
Unloads the Privileged Access Manager kernel extension from the kernel and then removes the module from streams.

#### NOTE

You cannot unload Privileged Access Manager if an application, which is loaded on top of Privileged Access Manager, has an open system call (syscall) that is hooked by Privileged Access Manager. Use *secons -sc* or *secons -sc/* to find these processes. You can then shut down these processes and unload the Privileged Access Manager kernel module, or use UNIX exits to automatically shut down these processes before unloading the kernel and then restart them after the kernel unloaded.

## sepass Utility Set or Replace a Password

### Valid on UNIX

The sepass utility sets a new password or replaces an existing password in the local host, in a Policy Model, or in the NIS or NIS+ server, as applicable.

The sepass utility changes the user password. Additionally, privileged users can use sepass to change the passwords of other users. When changing your own password, sepass prompts you for your old password.

#### NOTE

If seosd is not running, sepass runs a default password program. The DefaultPasswdCmd token in the passwd section of the seos.ini file specifies the default password program. Passwords are stored and transferred over the network in an encrypted format.

This command has the following format:

```
sepass [-d] [-l] [-p] [-s policy_model@hostname] \  
[-g number] [-x] [userName]
```

- **-d**  
Displays all the information it has regarding the password update, such as on which stations the update succeeded and if you did not activate setoptions class+(PASSWORD), that the password's quality was not checked. This switch is useful when debugging.
- **-g *number***  
Defines the number of grace logins for *userName*.
- **-h**  
Displays the help for this utility.
- **-l**



Replaces the password only on the local station; that is, in the local password file (usually `/etc/passwd`), security files, and the local database.

In the NIS/NIS+ environments, users are not usually defined in the `/etc/passwd` file of the client; therefore, the password on the client station is not updated.

In NIS/NIS+ server stations, the password is updated locally and propagated by NIS/NIS+.

This switch and the `-p` and `-s` switches are mutually exclusive.

- **-p**  
Changes the password only on the remote station and on the PMDB at the host specified in the switch. This switch and the `-l` and `-s` switches are mutually exclusive.
- **-s *policy\_model@hostname***  
Replaces the password on the local station and on the PMDB at the host specified in the switch. This switch and the `-l` and `-p` switches are mutually exclusive.
- **-x**  
Replaces the password as if changed by the user *username*. This switch updates the time and date of the last change in the database. Grace logins are terminated.

#### NOTE

To let you change the root password as if changed by root, you have to set the `RootPwAsOwn` appropriately. For more information about `seos.ini` tokens, see the *Reference Guide*.

- ***username***  
(Optional) Specifies the name of the user whose password `sepass` changes. If you omit this option, your own password is set.

## Examples

The following examples illustrate how you can use `sepass` in a variety of situations:

- To change your own password on the local host, enter the command:

```
sepass -l
```

#### NOTE

If no PMDB is defined at the site, you can omit the `-l` switch. If a PMDB is in use at the site, omitting the `-l` switch changes your password on all subscriber databases of the PMDB. In an NIS/NIS+ client, this switch *does not* change the password; in an NIS/NIS+ server, the password is changed and then propagated.

- To change the password of any user other than your own, on the local host only, enter the command:

```
sepass -l username
```

*username* must exist in the `/etc/passwd` file, the appropriate UNIX security files, and the database.

In an NIS/NIS+ client, `sepass` does not change the password. In an NIS/NIS+ server, the password is changed and then propagated.

- To change the password of a user on several stations at a site where NIS is not in use, follow these steps:
  - a. Create a PMDB.

#### NOTE

For more information about creating PMDBs, see the *Endpoint Administration Guide for UNIX*.

- b. Add all the users whose details must be distributed to the subscriber computers, to both the UNIX and the Privileged Access Manager environments of the PMDB.
- c. Subscribe all the stations to receive the updated passwords to the PMDB.
- d. On every subscriber, set the tokens in the `[seos]` section of the `seos.ini` file to the names of your PMDB. For example:

```
passwd_pmd = PMD1@morocco
```

```
parent_pmd = PMD1@casablanca
```

Enter the command:  
`sepass username` When `sepass` completes execution, the user's password is changed on all the subscriber databases.

## AM SC sepmd Utility

The sepmd utility is the Policy Model management utility, enabling you to perform the following tasks:

- Administer subscribers and the update file
- Administer Dual Control
- Manage the Policy Model log file
- Manage the PMDB
- Back up the PMDB
- Restore the PMDB

### NOTE

Run the sepmd utility on the host where the Policy Model resides.

Use the table of contents to access the topics in this section.

## sepmd Utility Administer Subscribers and the Update File

The sepmd utility creates, removes, and assigns subscribers.

This command has the following format:

```
sepmd {-C|-de|-l|-L|-p|-R} pmd
sepmd {-n|-r|-u} <pmd> <subscriber>
sepmd -s <pmd> <subscriber> <offset>
sepmd -sm pmdmf_subscribermf_typedmf_sysidmf_adminoffset
sepmd -smq pmd <-predefined> <ACMQ queue> [-destination <destination>]
sepmd -t pmd {auto|offset}
```

- **-C**  
This parameter displays all commands and their offsets in the update file. The offset indicates the location of the update inside the file, which you might want to specify when you subscribe another database or PMDB.
- **-de**  
(UNIX only) Decrypts the information in the encrypted updates.dat file. Data encryption for this file occurs when you set the UseEncryption PMDB configuration setting to yes.
- **-l**  
Lists the subscribers of the Policy Model.
- **-L**  
Lists the Policy Model and its status, including number of errors, availability, offset, synchronization mode, and the next command to be propagated. The update file contains all updates that must be, or have been, propagated by the Policy Model. The offset indicates the location of the next update that must be sent to a subscriber. Both initial and latest offsets also appear.
- **-n**  
Creates a new subscriber and then updates it retroactively to the Policy Model. For general rules that apply for updating a subscriber, see the description for the -s option.

### NOTE

This option sends the contents of the entire PMDB—including the LOGINAPPL (UNIX only) and SPECIALPGM objects—to the new subscriber. You might want to filter out these objects if the subscriber's objects differ from those of the parent.

The -n option does not replace the Policy Model database definitions on the target subscriber database definition, rather it is added to the existing Policy Model. If the target database contains additional resources or attributes, the new Policy Model does not remove them after subscription is complete.

A subscriber added with `-n` is marked as *sync*, indicating that it is now in synchronization mode and receives all of the PMDB rules. When the subscriber has received all the rules, it is released from synchronization mode and becomes a regular subscriber. The `-n` option might take some time to process. If there are multiple or contradictory updates, the last one is used.

### **WARNING**

When you subscribe a Privileged Access Manager endpoint or a PMDB to another PMDB using `sepmdb -n`, the new parent PMDB should not contain any policies (POLICY object names) that already exist in the new subscriber. Undeploy each existing policy from the subscriber and then delete the POLICY object and linked RULESET object from the subscriber before you subscribe it to the new parent PMDB.

On UNIX, if the `send_unix_env` token in the `seos.ini` file is set to yes, the `-n` option also sends the contents of Policy Model password and group files. We recommended that you view the database, by using `dbmgr -export -l`, to ascertain the commands being forwarded.

- **-p**  
Lists the resident Policy Models and their status.
- **-r**  
Removes the subscriber from the list of unavailable subscribers maintained by `sepmdd`, making the subscriber available for immediate updates. Normally, if a subscriber is down and cannot receive updates from the Policy Model, `sepmdd` tries to send updates to that subscriber only after a certain period of time. However, if you specify this option, `sepmdd` skips the waiting period and tries to send updates to the subscriber immediately.
- **-R**  
Update all subscribers with their real offset.
- **-s**  
Subscribes another database or PMDB to the Policy Model. When you subscribe a host to a Policy Model, the host must be up, and Privileged Access Manager must be running on that host. Additionally, the PMDB must be the parent PMDB of the subscribed host. You establish this relationship with the `parent_pmd` subscriber configuration setting, which must contain the name of the PMDB to which the host is being subscribed.  
When you subscribe a Policy Model to another Policy Model,
  - the token `parent_pmd` in the `pmd.ini` file of the subscribed Policy Model must contain the name of the Policy Model to which it is subscribing (its parent Policy Model).
  - Privileged Access Manager must be running on the host in which the subscribed policy resides.
 A PMDB should have only one parent. If you decide to establish a Policy Model with more than one parent give the `parent_pmd` token the name of a file containing a list of the parent Policy Models. However, establishing more than one parent is not recommended because you risk inundating your database with unreliable instructions from multiple sources.
- **-sm**  
Assigns a mainframe subscriber to the Policy Model.
- **-smq**  
Subscribes a pre-defined message queue subscriber to a policy model.
  - **<ACMQ queue>**  
Specifies the following pre-defined Message Queue queues:
    - a. ServerToServer
    - b. ServerToServerBroadcast
    - c. ServerToEndpointBroadcast
    - d. EndpointToServer
    - e. ServeryoEndpoint
  - **-destination**  
Specifies the destination of the Privileged Access Manager component that receives messages from the subscriber.
- **-t**  
Truncates the update file by deleting entries from it.

**NOTE**

On UNIX, if the `force_auto_truncate` PMDB configuration setting is set to no, `sepmc -t` does not truncate the update file. If the token is set to yes, the command truncates the update file even if there are no subscribers to the Policy Model.

- If you are using *offset* (manual cutting), you can find the offset by running `sepmc` with the `-L` option.

**NOTE**

Use the true offset from the `-L` parameter to truncate the file, and not an offset derived by subtracting from the start offset.

- If you are using *auto*, `sepmc` calculates the offset of the first unpropagated entry and deletes all the entries before it. Using *auto* saves the step of running the utility with the `-L` parameter.

If a subscriber received fewer than all updates before the specified offset, `sepmc` displays an error message and does not truncate the file. If you want to truncate the file anyway, do the following:

- Unsubscribe the host that was not updated
- Truncate the file
- Resubscribe the host to the Policy Model

If you do this, the subscriber fails to receive one or more updates from the Policy Model. The subscriber's offset changes to the last offset of the updates file.

- **-u**  
Removes a subscriber from the Policy Model subscription list.
- **auto**  
Instructs `sepmc` to calculate the offset of the first unpropagated entry and to delete all the entries before it.
- **offset**  
Used with the `-s` or `-sm` options, specifies the point within the update file from where the newly added subscriber starts receiving updates.  
Used with the `-t` option, specifies the distance from the beginning of the update file to the position of a particular subscriber.  
Use the `-C` option to see the valid update offsets. If you specify an offset that is in the middle of an update, the offset is moved forward to the beginning of the next update. If you specify an invalid offset (smaller than the first offset or larger than the last), an error message appears.
- **pmd**  
Specifies the name of the Policy Model.
- **-predefined**  
Specifies to use pre-defined message queue subscribers
- **subscriber**  
Specifies the subscriber station or the host of the subscriber PMDB.

## sepmc Utility Administer Dual Control

### Valid on UNIX

The `sepmc` utility manages Dual Control transactions. The `sepmc` utility gives a unique ID number to each transaction when it is created.

**NOTE**

For more information about Dual Control, see the *Endpoint Administration Guide for UNIX*.

When you use Dual Control, the name of the PMDB must be *maker* and the `is_maker_checker` configuration setting must have the value yes for both the PMDB and Privileged Access Manager.

This command has the following format:

```
sepmc -m {1|1a|1o}
```

```
sepmdd -m {d|r} <transactionId>
sepmdd -m p <transactionId> <code>
```

- **-m d**  
Deletes the transaction. A transaction is one or more commands that must be approved before they are implemented on the PMDB. Only the user who created the transaction can delete it.
- **-m l**  
Lists the unprocessed transactions (awaiting the Checker) of the user who invoked the command. Each transaction is listed with its ID number, the name of its Maker (the user who created the transaction-in this case the same user who invoked the command), and its description, if any.
- **-m la**  
Lists all the unprocessed transactions of all the Makers. Each transaction is listed with its ID number, the name of its Maker, and its description, if any.
- **-m lo**  
Lists the unprocessed transactions (awaiting the checker) of all the Makers *except* the transactions of the user who invoked the command.
- **-m p**  
Processes a transaction. When the Checker (any admin user *except* the Maker who created the transaction) enters an ID number, all the commands in the specified transaction appear in a list.  
This option does not work in the following circumstances:
  - If one or more of the commands in the transaction pertain to the user who invoked the command.
  - If the transaction is locked by a different Checker
  - If the transaction was created by the user who invoked the command-Makers cannot act as Checkers for their own transactions.
  - If the specified transaction ID does not exist.
  - If the user who invokes the command does not have the authority to be a Checker.
- **-m r**  
Retrieves or locks a transaction.
  - If you are the user who created the transaction (the Maker) this parameter retrieves a specific, unprocessed transaction. After you retrieve the transaction, you can direct it to an appropriate file and use the ASCII editor of your choice (vi, emacs, and so on) to update the transaction.
  - If you are a user who is *not* the Maker (Checker) this parameter locks the transaction before processing. You cannot change a locked transaction.
- **transactionID**  
Specifies the unique identifying number that sepmdd gives to the transaction when it is created
- **code**  
Specifies a numeric code that tells the Checker what to do when processing the transaction:
  - **0**  
Rejects the transaction, in which case all the commands in the transaction are deleted and no changes are implemented in the PMDB
  - **1**  
Authorizes the transaction, in which case the commands are immediately implemented in the PMDB
  - **2**  
Unlocks the transaction so that it can be processed later, or by a different Checker.

## sepmdd Utility Back Up the PMDB

The sepmdd utility lets you back up the Policy Model database.

This command has the following format:

```
sepmdb {-bl|-ul} pmd
sepmdb -bd <pmd> <destination>
sepmdb -bh <pmd> <destination> <backup_host>
```

- **-bd**  
Backs up *pmd* to the directory *destination*.
- **-bh**  
Backs up *pmd* to the directory *destination* for Policy Models in a hierarchy. The backup modifies the PMDB subscribers so that the subscription still works when the backup is moved to the *backup\_host* host.
- **-bl**  
Locks the *pmd* so that it does not propagate commands to subscribers.  
Use this command if the Policy Model has subscribers and you want to ensure that updates are not accepted while the backup is in process.
- **-ul**  
Unlocks a locked *pmd*
- **backup\_host**  
Defines the name of the host where you intend to move the backup host to
- **destination**  
Defines the name of the directory where you want the PMDB files to be backed up to
- **pmd**  
Defines the Policy Model database, which is located where specified by the `_pmd_directory_` configuration setting.

### Example: Back Up a PMDB

The following command backs up a PMDB named myPMDB to the /tmp/my\_pmdb directory:

```
sepmdb -bd pmdb /tmp/my_pmdb
```

You can now manage the PMDB as required:

```
selang -d /tmp/my_pmdb
```

### Example: Back Up a PMDB with Subscribers

The following commands show you how to back up a PMDB that has subscribers and then move the PMDB to a different host:

1. Lock the PMDB:

```
sepmdb -bl mainPMDB
```

Privileged Access Manager locks the PMDB so that it does not send or receive updates.

2. Back up the PMDB:

```
sepmdb -bh mainPMDB /tmp/my_pmdb host63
```

Privileged Access Manager backs up the PMDB to the /tmp/my\_pmdb

On UNIX, Privileged Access Manager updates subscribers.dat with the backup host name you specified.

On Windows, Privileged Access Manager creates a *pmd.reg* file, which is a dump of the *pmd* registry settings with the Parent\_Pmd configuration setting value changed to match the new host you specified.

3. Unlock the PMDB:

```
sepmdb -ul mainPMDB
```

Privileged Access Manager unlocks the PMDB.

4. Transfer the PMDB backup to its new host.

#### NOTE

The new host must have the same OS and Privileged Access Manager version as the current computer.

5. (Windows only) Import the mainPMDB.reg file into the registry on the new host.

You can now continue to use the PMDB as you typically would.

## sepmdd Utility Manage the Policy Model Log File

The sepmdd utility manages the Policy Model log file. The Policy Model log file provides a detailed audit trail of Policy Model data base activities. For example:

```
Wed Nov 4 10:08:02 2003 pmdb1:Processing list request for missouri.yourco.com
Wed Nov 4 10:08:02 2003 pmdb1:Processing list request for oregon.yourco.com
Wed Nov 4 10:09:14 2003 pmdb1:Empty request
Wed Nov 4 10:09:15 2003 pmdb1:Processing shutdown request
Wed Nov 4 10:09:15 2003 pmdb1>Delete filters
Wed Nov 4 10:10:04 2003 pmdb1:Opened error logs
Wed Nov 4 10:10:04 2003 pmdb1:Try to load filters
Wed Nov 4 10:10:04 2003 pmdb1:Filters file : nis_filter.dat
```

Running sepmdd for the first time automatically creates the Policy Model log file.

On UNIX, use the pmd\_log\_level PMDB configuration setting to control the PMDB logs:

- **0** - Do not log any entries
- **1** - List only error messages
- **2** - List error and informational messages (default value)

### NOTE

A warning message in the log file tells you whether you have exceeded file size limitations. Use configuration settings to increase the size of the log file. Privileged Access Manager does not rename (rotate) the pmd\_log file automatically.

This command has the following format:

```
sepmdd {-sl|-kl|-dl|-cl} pmd
```

- **-cl**  
Clears the contents of the Policy Model log file
- **-dl**  
Displays the Policy Model log file
- **-kl**  
Makes the Policy Model log file unavailable
- **-sl**  
Makes the Policy Model log file available
- **pmd**  
Specifies the name of the Policy Model

## sepmdd Utility Manage the PMDB

The sepmdd utility stops and starts Policy Models. On UNIX, it also reloads configuration settings that affect the Policy Model.

### NOTE

In Windows, unlike UNIX, sepmdd does not stop or start the Policy Model service. Instead, it activates and deactivates the Policy Model.

You must have ADMIN authority in the Policy Model to use sepmdd for starting or querying the Policy Model.

This command has the following format:

```
sepmdd {-c|-e|-k|-S} pmd
sepmdd -tm seconds
```

- **-c**  
Clears the Policy Model error log
- **-e**  
Displays the Policy Model error log
- **-k**  
On UNIX, this shuts down the Policy Model daemon safely. On Windows, it deactivates the Policy Model service.

**NOTE**

Do not use the kill command on UNIX to shut down the Policy Model daemon.

- **-ri**  
On UNIX, it reloads the Policy Model and Privileged Access Manager configuration files (pmd.ini and seos.ini respectively) while sepmd is running. You can only use this option at intervals of one minute or more. This option checks configuration changes in the following tokens: parent\_pmd, \_retry\_timeout\_, \_min\_retries\_, and \_shutoff\_time\_.  
On Windows, it reloads Policy Model information from the registry to the hosts. Use this switch if you changed data and want to be sure that it is sent to the host PMDBs.
- **-S**  
On UNIX, starts the Policy Model daemon. On Windows, it activates the Policy Model service.  
Use this option to start the daemon when you do not have any other commands to execute.
- **-tm seconds**  
(Windows only) Sets an initial timeout interval (in seconds) for the executed request.
- **pmd**  
Specifies the name of the Policy Model

## sepmd Utility Restore the PMDB

The sepmd restores a PMDB on a local host. The backup files that you use to restore the PMDB must be from a host running the same platform, operating system, and version of Privileged Access Manager as the restoration host. Privileged Access Manager must be running on the restoration host.

**NOTE**

If you back up and restore the PMDB on different terminals, the PMDB does not automatically update the terminal resource in the restored PMDB database. Add the new terminal resource to the restored PMDB. To add the new terminal resource, stop the restored PMDB, run the *selang -p pmdb* command, then start the restored PMDB.

This command has the following format:

```
sepmd -restore pmd [-source path] [-admins user[,user...]] \
[-xadmins user[,user...]] [-parent_pmd name[,name...]]
```

- **-restore**  
Restores the PMDB on the localhost
- **-admins user[,user...]**  
(UNIX) Defines internal users as administrators of the restored PMDB.
- **-parent\_pmd name[,name...]**  
(Optional) Defines the name of the restored PMDB parent PMDBs. Specify the parent PMDB name in the format *pmdb@host*.
- **pmd**  
Defines the name of the PMDB to restore
- **-source(path)**



(Optional) Defines the directory where the backup files are located. The path is required as a full path. If you do not specify the source directory, the PMDB is restored from the files in the default location. The default location is defined in the `_pmd_backup_directory_` token.

**NOTE**

**Default:** (UNIX) `ACInstallDir/data/policies_backup/pmdNameDefault`: (Windows) `ACInstallDir\data\policies_backup\pmdName`

- **-xadmins *user[,user...]***  
(UNIX) Defines enterprise users as administrators of the restored PMDB.

## sepmdbadm Utility Create PMDB Definitions

### Valid on UNIX

The `sepmdbadm` utility creates the definitions to run a PMDB. The `sepmdbadm` utility is a script consisting of Privileged Access Manager and the required UNIX commands to define a PMDB, to define the relationship of the PMDB to PMDBs above and below it, and to define its subscriber stations. By default, the user root is defined as the administrator and auditor of the PMDB. Run the `sepmdbadm` utility locally. You can run it through a remote shell. When you use `sepmdbadm` to create a PMDB, point subscribers to the PMDB and synchronize the UIDs and GIDs.

You can run this utility in interactive or non-interactive modes:

- In non-interactive mode, you enter arguments in the command line. The utility builds the PMDB and its hierarchy according to the values it receives.
- In interactive mode, you do not enter arguments in the command line. The `sepmdbadm` utility asks the user if the desired mode is interactive. If the user answers y, then the utility proceeds to ask the user for option values.

When creating a PMDB with `sepmdbadm`, you identify the stations that are the subscribers of the Policy Model. Update the `parent_pmd` token in each subscriber `seos.ini` file with the name of the PMDB to which you have subscribed the station. If you do not do this, the subscribers do not accept updates from the PMDB.

By subscribing several stations to the same PMDB, and by subscribing one PMDB station to another, you can create a hierarchy of PMDBs.

This command has the following format:

```
sepmdbadm options
```

- **--admin *name***  
Defines the Privileged Access Manager administrator of the PMDB
- **--auditor *name***  
Defines the Privileged Access Manager auditor of the PMDB
- **-c | --clean *pmdbName***  
Removes the specified Policy Model. This option shuts down the Policy Model daemon, removes the file protections from the database, and deletes the Policy Model directory with all its contents.  
You cannot use this option with the `--noconfirm` option.
- **--desktop *hostname***  
Specifies a station from which the administrators can administer PMDBs on the local host. If you do not specify any stations, the administrators can only administer the PMDBs from the local host.
- **--group\_fname *fileName***  
Defines the location of the groups file under NIS
- **-h | --help**  
Displays the help screen
- **-i | --interactive**  
Runs `sepmdbadm` in interactive mode
- **-l**

Specifies to run sepmdadm in local mode, meaning that you can create a PMDB when Privileged Access Manager is not running.

#### NOTE

Unless you specify this option you must have Privileged Access Manager running to use sepmdadm.

- **--nis | --NIS**  
Performs NIS setup on the Policy Model. Use this option if the PMDB is installed on a NIS server.
- **--noconfirm**  
Specifies that the user is not asked to confirm answers. This option is useful when invoking sepmdadm from within a shell script in non-interactive mode.
- **--parentpmd *pmdbName***  
Specifies the name of the parent PMDB to which this PMDB is subscribed. If you use this parameter with the -subsconfig parameter, sepmdadm updates the parent\_pmd token in the seos.ini file. If you use this parameter without the --subsconfig parameter, sepmdadm updates the parent\_pmd token in the pmd.ini file.

#### NOTE

If you want to define multiple parent Policy Models, you must to use quotation marks. For example, to create a Policy Model and define its parent, use the following command:

```
sepmdadm --pmdname subs2 --admin abc123 --admin root --auditors abc123 --desktop pcp36949 \
--parentpmd "aa@pcp36949,bb@pcp36949"
```

- **--passwd\_fname *fileName***  
Defines the location of the passwd file under NIS
- **--passwdpmd *pmdbName***  
Specifies the PMDB to which sepass sends password updates. This option updates the passwd\_pmd token in the [seos] section of the seos.ini file.

#### NOTE

You can use this parameter only when you also use the --subsconfig switch.

When creating a multi-level Policy Model, set this parameter to the PMDB at the top of the pyramid, so that password changes can be propagated to all levels in the PMDB system.

- **--pmdname *pmdbName***  
Specifies the name of the PMDB to be created
- **--pwmanager *name***  
Specifies the Privileged Access Manager password manager of the PMDB
- **--seosdir *directory***  
Specifies the directory in which Privileged Access Manager is installed. Use this option only if Privileged Access Manager is not installed in the default directory.
- **--subsconfig**  
Specifies that the local station is a subscriber. When using this parameter, you must specify the parameters --parentpmd *pmdbName* and --passwdpmd *pmdbName* to update the relevant tokens in the seos.ini file.

#### NOTE

The parameters should follow the -subsconfig option when configuring a subscriber.

- **--subscriber *name***  
Specifies subscribers of this PMDB. They can be PMDBs or stations
- **--xadmin *name***  
Defines the enterprise user administrator of the PMDB
- **--xauditor *name***  
Defines the enterprise user auditor of the PMDB
- **--xpwmanager *name***  
Specifies the enterprise user password manager of the PMDB

### Example: Create a PMDB using the command line

Suppose that you have a station named bigcentral, where you want to maintain a PMDB for other stations to subscribe to. To create the PMDB at bigcentral, run sepmdadm there. This utility is located in the directory *ACInstallDir/bin*.

To create a PMDB on bigcentral named pmdb1 with workstat1 and workstat2 as subscribers and enterprise users adm1 and adm2 as administrators, run the following command from bigcentral:

```
sepmdadm --pmdname pmdb1 --subscriber workstat1 --subscriber workstat2 \
--xadmin adm1 --xadmin adm2
```

### Example: Pointing subscriber stations to the PMDB

To establish a station as a subscriber to a PMDB, it is not sufficient to specify the subscriber name at the PMDB station. Perform a procedure at the subscriber station also.

To subscribe the local station to a PMDB using the command line, use the parameters --parentpmd and --passwdpmd, in addition to the parameter --subsconfig.

For example, to subscribe the local station to the PMDB named pmdb2 on HOST2 and to the password PMDB named master1 on HOST1, enter the following command:

```
sepmdadm --subsconfig --parentpmd pmdb2@HOST2 --passwdpmd master1@HOST1
```

## sepropadm Utility Administer Database Properties

The sepropadm utility adds, updates, and deletes properties in the database. Invoke this utility from the directory in which the database resides, and while Privileged Access Manager is *not* running. The sepropadm utility can add only one property at a time.

### WARNING

This utility is for Privileged Access Manager technical support personnel use only. Use sepropadm only with a description file that was certified by Privileged Access Manager technical support personnel.

This command has the following format:

```
sepropadm file
```

- **file**

Specifies a description file that is supplied by Privileged Access Manager support personnel. The description file uses the following format:

- There must be one line that begins with the hash symbol (#); it must precede the description lines.
- Lines that begin with semicolon(;) are comments and are not processed.
- The description line to add a new double link OID must conform to the following format:

```
CLASS=%s    PROPERTY=%s    TYPE=%d    SIZE=%d    FLAGS=%x
```

- The description line to add a new property must conform to the following format:

```
CLASS=%s    PROPERTY=%s    TYPE=%d    SIZE=%d    FLAGS=%x    LINK2CLASS=%s
```

- The description line to delete a property must conform to the following format:

```
CLASS=%s    PROPERTY=%s
```

- The description line to change a property must conform to the following format:

```
CLASS=%s    PROPERTY=%s    TYPE=%d    SIZE=%d    FLAGS=%x    REPLACE=YES
```

### Example: A description file for sepropadm

The following is a sample description file.

```
; Sample Patch File for the CA PAMSC database
```

```
; Copyright YYYY CA International, Inc.
```

```
; -----
```

```
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
```

```
# seclassadm database add property patch utility ; Format is : CLASS=PROGRAM PROPERTY=MD5 TYPE
```

## sepromote Utility Enforce Strong Authentication

Privileged Access Manager integrates with Advanced Authentication to provide a strong authentication option for privileged and other native users of the operating system.

The Privileged Access Manager system administrator restricts interactive sessions coming from a terminal by adding users to a group. To get write permission to files, users in this group must authenticate themselves using CA ArcotID OTP (one-time passwords).

After authentication, Privileged Access Manager does not apply the rules that are created for the native user (root), but it applies rules to users according to their internal identities. Privileged Access Manager differentiates non-restricted, restricted, and promoted users, and applies specific rules to them.

- When a user *name* from the `interactive_restricted` group logs in interactively, Privileged Access Manager identifies him as "`restricted_name`".

#### Examples:

- When root logs in interactively, Privileged Access Manager applies the rules for the user "`restricted_root`" (if specified) or otherwise "`_default`" restricted rules.
- When root logs in non-interactively, Privileged Access Manager applies the rules for the root user.
- When a user from the `interactive_restricted` group promotes himself with an enterprise name, Privileged Access Manager identifies him as "*name2*".

#### Example:

- When root promotes as "*name2*", Privileged Access Manager applies the rules for the user "*name2*".

This command has the following format:

```
sepromote [-h] [-u username] [-o orgname] [otp] [-v]
```

- **-h**  
Displays help and exits.
- **-u *username***  
Defines the name of the user in the `interactive_restricted` group who is requesting strong authentication.

**Default:** If not supplied as argument, the tool prompts for the user name.

- **otp**  
Defines the one-time password that the user in the interactive\_restricted group has generated.  
**Default:** If not supplied as argument, the tool prompts for the password.
- **-o orgname**  
Defines the organization where Advanced Authentication searches users of strong authentication.  
**Default:** Value of the organization\_name token in [strong\\_auth](#).
- **-v**  
Activates verbose mode.

## sepurgdb Utility Purge Database References to Undefined Records

### Valid on UNIX

The sepurgdb utility searches the entire database for references to undefined records, and then deletes those references from the database, reducing the size of the database.

#### WARNING

For safety purposes, back up the database, and then invoke the utility while the Privileged Access Manager daemons are *not* running.

When a record is deleted, references to it in lists such as ACLs or group membership lists are left as is, to reduce processing time. This does not cause any problems, because Privileged Access Manager assigns a previously unused, unique ID to each new record. Use this utility to free up some disk space.

Run sepurgdb as root and invoke the utility from the directory containing the database files. The database management system uses pre-allocated disk space. The size of the database file typically does not change significantly after purging. When the size of the database is increased later, the file size might not change due to the pre-allocation.

This command has the following format:

```
sepurgdb FilePath [Username]
```

- **FilePath**  
Specifies the base name for the utility log files. The sepurgdb utility creates two log files:
  - **FilePath.err**  
Contains a log of errors encountered
  - **FilePath.log**  
Contains a log of actions taken

#### NOTE

You can merge the two logs and direct them to the standard output by specifying a minus sign (-) for *FilePath*.

- **Username**  
(Optional) Specifies the name of the user that sepurgdb uses to replace deleted owners (users that no longer exist) of the group connection for the USER record.

#### NOTE

The user that you define must exist in the database, otherwise the utility ignores this option.

## sereport Utility Reports Configuration

The sereport utility provides HTML reports, accessible from a web browser, of database and Policy Model information. sereport operates on the current database that is used by the authorization engine.

You can set sereport options for the utility:

- On UNIX, sereport uses a configuration file that you specify using the -f option.  
By default, this setting is *ACInstallDir/etc/sereport.cfg*
- On Windows, sereport uses the registry, which you can configure. The registry settings for sereport are defined under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Report

The reports that you can generate, their description and corresponding configuration file settings or registry keys are shown in following table.

Report Number	Title and Description	Section\Subkey	Tokens\Entries
1	Administrative Privileges Display specified administrative privileges of users.	admin_report	Hostname Objects_Pattern User_Mode
2	Login Limitation Display login limitations of users.	disablelogins_report	Hostname Objects_Pattern Properties User_Mode
3	Dormant Accounts Display inactive accounts by date (days). If an account does not have any login information, the create time is used to calculate dormant days.	dormant_report	Hostname Objects_Pattern Dormant_account User_Mode
4	Last Login Display last login date of users.	login_report	Hostname Objects_Pattern User_Mode
5	Password Change Display list of users whose passwords must be changed within the specified number of days.	passwd_report	Days_to_change Hostname Objects_Pattern User_Mode
6	Warning Mode Display resources with objects in warning mode.	warning_report	Class_Name Hostname Objects_Pattern
7	Untrusted Programs Display programs in untrusted mode.	untrust_report	Hostname Objects_Pattern
8	Users Privilege Access Rights Show access privileges of users to specified resources.	accessor_report	Accessor Class_Name Hostname Objects_Pattern
9	Compare users/groups in databases. Display users and groups that are defined in some but not all, databases.	grp_usr_compare	Hostname Objects_Pattern

10	Compare Protected Resources Display whether resources are defined in the specified databases.	res_compare	Class_Name Hostname Objects_Pattern
11	Compare Access Rights Display the differences in resource restrictions between a Policy Model and a subscriber database.	acc_compare	Class_Name Hostname Objects_Pattern
12	Compare Users Information Display differences in user definitions between a Policy Model and a subscriber database.	usr_compare	Hostname Objects_Pattern Properties
13	Compare PMDB and Subscriber Display the rules (as defined by the Class_Name and Object_pattern tokens) that exist on the PMDB, but do not exist on the subscriber database. Note: If all the rules on the PMDB exist on the subscriber database, then the databases are reported as IDENTICAL.	pmdb_compare	Class_Name Hostname Objects_Pattern

- **Accessor**  
Specifies the pattern (mask) for accessor selection. Use \* to select all accessors
- **Class\_Name**  
Specifies a list of classes
- **Days\_to\_change**  
Specifies the number of days that are left until the user is requested to change passwords
- **Dormant\_account**  
Specifies the period that the account is considered dormant
- **Hostname**  
Specifies a list of hosts from which the data is retrieved
- **Objects\_pattern**  
Specifies the pattern (mask) for object selection. Use \* to select all objects.
- **Properties**  
Specifies attributes that are associated with the objects
- **Report\_place**  
(UNIX only) Specifies the full path location where the report is printed.

**NOTE**

On Windows, you define the location of the output using the -f option of the command.

- **User\_Mode**  
Specifies a comma-separated list of user modes

You can also find the following configuration settings in the colors section\key:

- **title**  
Specifies the color of the report title
- **class\_title**

Specifies color of the report class\_title

- **background**  
(UNIX only) Specifies the color of the title report background. The background and logo must be written in full path.
- **logo**  
Creates the logo. The background and logo must be written in full path.

## sereport Utility Create HTML Reports on UNIX

### Valid on UNIX

The sereport utility creates HTML reports, accessible from a web browser, of database and Policy Model information. sereport operates on the current database that is used by the authorization engine.

To use sereport, you need READ privileges in all queried databases.

#### NOTE

The default configuration file is *ACInstallDir/etc/sereport.cfg*

This command has the following format:

```
sereport [-f|-file pathname] -r|-report number [-host hostnames]
```

- **-f | -file *pathname***  
(Optional) Specifies the full path of the configuration file. If you do not specify a file, sereport uses the default file *ACInstallDir/etc/sereport.cfg*
- **-host *hostnames***  
(Optional) Specifies the names of one or more hosts you want to report on. If you do not specify a host, sereport takes the host from the config file.
- **-r | report *number***  
Specifies the report number to create

## sereport Utility Create HTML Reports on Windows

### Valid on Windows

The sereport utility creates HTML reports, accessible from a web browser, of database and Policy Model information. sereport operates on the current database used by the authorization engine.

To use sereport, you need READ privileges in all queried databases.

This command has the following format:

```
sereport -f|-file pathname-r|-report number [-host hostnames]
```

- **-f | -file *pathname***  
Specifies the full pathname of the output file (the report).

#### NOTE

The content of the specified file is structured in HTML format so you should specify the *.html* extension for automatic file association.

- **-host *hostnames***  
(Optional) Specifies the names of one or more hosts you want to report on. If you do not specify a host, sereport uses *localhost*.
- **-r | report *number***  
Specifies the report number to create.



## seretrust Utility Generate Commands to Retruster Programs and Secure Files

The seretrust utility generates the selang commands that are required to retrust programs and secure files that are defined in the database. The seretrust utility reports the status of the SECFILE and PROGRAM resources that are defined as trusted but have changed. seretrust also checks whether programs have been changed but have not yet been caught by the Watchdog. (This means that in the Privileged Access Manager database, these programs are still marked as trusted.) These programs are added to seretrust output with a note stating that the program content or timestamp has been changed, and to retrust the program.

### NOTE

On UNIX, programs with setuid and setgid bits are stored in the database with full descriptions, including inode values. If you restore the system from backups, the programs occupy different inodes. Privileged Access Manager detects the mismatch between the inodes and marks all the trusted programs as untrusted. The seretrust utility locates the trusted programs that are defined in the database and updates their inode values, so that when you invoke Privileged Access Manager, the trusted programs remain trusted.

If you do not specify any switches, only untrusted programs and untrusted secured files are processed.

This command has the following format:

```
seretrust [-a] [-l|-m|-p|-s] path
```

- **-a**  
Processes all trusted and untrusted objects.
- **-h**  
Displays the help for this utility
- **-l**  
Extracts information about the programs and files from the database in the current directory.  
If you omit this option, seretrust processes the database that Privileged Access Manager uses.
- **-m**  
Calculates the signatures for all kernel modules. If the signature property of a kernel module record is not valid, seretrust updates it with the correct signature, which ensures that the kernel module is trusted. Signatures are used only for Linux kernel modules.
- **-p**  
Processes records in the PROGRAM class only
- **-s**  
Processes records in the SECFILE class only
- *path*  
Specifies the base path for searching programs and secure files to retrust.  
The utility processes the specified directory and all subdirectories.

### Example: Retruster untrusted programs and secure files

This example shows you how you can use the seretrust utility to retrust programs and secure files.

### NOTE

This example shows you a sample command output on UNIX, but the utility works the same on Windows.

To retrust programs and secure files, follow these steps:

1. As the Privileged Access Manager database administrator, enter the following seretrust command:

```
seretrust > retrust_script
```

The utility processes both trusted programs and secured files because you did not specify any options. It also uses the root path because you did not specify any base path.

seretrust displays the following information about the screen:

```
Retrusting PROGRAMs & SECFILEs, Base path = /
Total of 0 entries retrusted. (Class=SECFILE)
```

Total of 16 entities retrusted. (class=PROGRAM)

The following code is the content of a script file `seretrust` can create:

```
chres PROGRAM ("/usr/bin/chgrp") trust
chres PROGRAM ("/usr/bin/chie") trust
chres PROGRAM ("/usr/bin/crontab") trust
chres PROGRAM ("/usr/bin/cu") trust
chres PROGRAM ("/usr/bin/ecs") trust
chres PROGRAM ("/usr/bin/newgrp") trust
chres PROGRAM ("/usr/bin/rmqudev") trust
chres PROGRAM ("/usr/bin/rsh") trust
chres PROGRAM ("/usr/bin/sysck") trust
chres PROGRAM ("/usr/bin/uuname") trust
chres PROGRAM ("/usr/lib/methods/showled") trust
chres PROGRAM ("/usr/lib/mh/post") trust
chres PROGRAM ("/usr/lib/mh/slocal") trust
chres PROGRAM ("/usr/lpp/X11/bin/xlock") trust
chres PROGRAM ("/usr/lpp/X11/bin/xterm") trust
chres PROGRAM ("/usr/sbin/chvprt") trust
```

2. Run the `selang` script file `seretrust` created to retrust the programs and files:

```
selang -f retrust_script
```

## serevu Utility Handle Unsuccessful Login Attempts

### Valid on UNIX

The `serevu` utility handles users who have had a specified number of failed login attempts during a specified period. Depending on your specifications, it can disable, report, or ignore the user. By default, it disables the user in the UNIX environment of the local station. If no such user exists locally, `serevu` checks the NIS information to find the user.

If you set a value in the `passwd_pmd` configuration setting, Privileged Access Manager updates the appropriate PMDB, which then propagates the update to its subscribers. If you did not set a value in the `passwd_pmd` token, Privileged Access Manager uses the value in the `parent_pmd` configuration setting, which then propagates the update to its subscribers.

**Note:** If you want `serevu` to send commands to the PMD (which, you can configure in `serevu.cfg`) and `root` is not defined on the PMD with the `ADMIN` attribute or with terminal access, you should define the following on the PMD and all of its subscribers:

```
eu _serevu logical
authorize admin USER uid(_serevu) access(a)
# The following line can be executed on the master PMD only
authorize terminal localTerminalName uid(_serevu) access(a)
```

### NOTE

For the `serevu` utility to work properly, the user `root` must have write access to the file `/etc/passwd`. If you define a remote computer in the `serevu` configuration file (`serevu.cfg`), you must also give login authorization to the remote computer. For example:

```
eu _serevu admin logical
authorize terminal localTerminalName uid(_serevu) access(a)
er specialpgm $ACDIR/bin/serevu seosuid(_serevu) unixuid(root)
```

This command has the following format:

```
serevu {daemon|nodeamon} [-f nn] \
```

```
[ -d {nn[s|m|h|d|w]|FOREVER} ] \
[ {-s|-t} nn[s|m|h|d|w] ]
```

- **daemon**  
Runs the utility as a daemon. This is the default value.
- **nodaemon**  
Runs the utility as a regular process.
- **-d**  
Specifies the amount of time for which the user's login is disabled. By default, this value is in seconds.

**NOTE**

The amount of time a user account is disabled cannot be less than the amount of time between each serevu scan. The amount of time a user account is disabled should be a multiple of the time between each serevu scan.

- **-f**  
Specifies the number of failed logins. The serevu utility disables the accounts of users who reach this number of failed logins over the specified period.

**NOTE**

We recommend that the number of failed logins, which can also be defined by the value of the *def\_fail\_count* configuration setting, always be the same as the value of allowed unsuccessful login attempts set on your system. (On Solaris, for example, the system values for this are set in */etc/default/login* by the RETRIES token.) See your operating system documentation for more details.

- **-h**  
Displays the help for this utility.
- **-s**  
Specifies the time period, starting from *now* and going backwards, within which serevu scans for failed logins.  
**Default:** 300 seconds (configuration setting).
- **-t**  
Specifies the time period that should elapse between successive serevu checks.  
**Default:** 120 seconds (configuration setting).
- **FOREVER**  
Used with the -d option, specifies the time as unlimited. If you use this parameter, user logins will be disabled forever.
- **nn[s|m|h|d|w]**  
Used with the -d, -s, and -t options, specifies the time for the option.
  - **s**  
nn in seconds (the default).
  - **m**  
nn in minutes.
  - **h**  
nn in hours.
  - **d**  
nn in days.
  - **w**  
nn in weeks.

## sesu Utility Substitute User

The sesu utility lets you temporarily act as another user. This utility is the Privileged Access Manager version of the UNIX su command. However, the sesu utility provides a user substitution command that does not require you to provide the password of the substituted user. The authorization process is based on the Privileged Access Manager access rules as defined in class SURROGATE and, optionally, on the password of the user executing the command.

The `sesu` utility uses the tokens in the `sesu` section of the `seos.ini` file. It also uses the following special files:

- `/etc/passwd`
- `/etc/group`
- `/etc/shells`

To protect against inadvertent use, `sesu` is marked in the file system so that no one can run it. The security administrator must mark the program as executable and `setuid` to root before you can use it.

### WARNING

Before you use the `sesu` utility, define all users to the Privileged Access Manager database and set `sesu` prerequisites. This prevents you from opening up the entire system to users who are not defined to Privileged Access Manager.

The `sesu` utility optionally supports strong authentication and can prompt the user for a one-time password. Activate strong authentication in the `sesu` and `strong_auth` sections of the `seos.ini` file.

**Note:** For more information about strong authentication and the `sepromote` utility, see [sepromote Utility Enforce Strong Authentication](#).

Usage notes:

- If the Privileged Access Manager authorization server is not found, the utility executes the system standard `su` command.
- If the `sesu.old_sesu` configuration token is set to `no`, the utility executes the system standard `su` command.
- If `/etc/shells` exists, and it does not specify the current shell, `sesu` does not permit substitution to root.

This utility has the following format:

```
sesu [-] [username] [-l] [-n] [-s shell] [-c command]
```

- **-**  
Sets the environment to that of the target user.
- **NOTE**  
On Linux, this is the same as using the `-l` option.
- **-c *command***  
Executes the specified command then exits  
Enclose commands containing spaces in quotes.
- **-h**  
Displays the help for this utility
- **-l**  
(Linux only) Specifies that the shell it opens is a login shell
- **-n**  
Specifies not to prompt the user for password

### WARNING

When used, the utility runs as the root account and performs a LOGIN event.

### NOTE

If the security authorization server is not found, the utility uses `/bin/su`.

- **-s *shell***  
(Linux only) Specifies a shell to open instead of the shell from the user `passwd` entry  
The shell must be listed in the `/etc/shells` file.
- ***username***  
Changes the ID associated with the session to the ID of the specified target user *username*  
If you do not specify a *username*, `sesu` default to root.

## Examples

- The following command changes the UID to root. The environment remains that of the user who executed the command.

```
sesu
```

- The following command changes the UID to root. The utility changes the environment to root environment.

```
sesu -
```

- The following command surrogates to the user John.

```
sesu John
```

- The following command surrogates to the user Carol and executes the specified command, `ls -la`, from the `/home/carol` directory.

```
sesu - Carol -c "ls -la /home/carol"
```

- The following command surrogates to the user Angelo, uses a bash shell, and opens it as a login shell.

```
sesu Angelo -l -s /bin/bash
```

### NOTE

This code is valid on Linux only.

## sesudo Utility

The `sesudo` utility executes commands for one user with the permissions of another user. This lets regular users perform actions that require administrator authority.

The rules governing user authority to perform commands in this way are defined as access rules in the SUDO class. A record in the SUDO class contains a command script, and can specify both users who are permitted to run the script with `sesudo` and users who are forbidden to.

## sesudo Utility Execute a Command as Another User on UNIX

### Valid on UNIX

The `sesudo` utility executes commands for one user with the permissions of another user. The `sesudo` utility borrows the permissions of another user (the *target* user) to perform one or more commands. This allows regular users to perform actions such as the `mount` command, which require superuser authority.

The rules governing user authority to perform commands in this way are defined as access rules in the SUDO class. A record in the SUDO class contains a command script, and can specify both users who are permitted to run the script with `sesudo` and users who are forbidden to.

Each time `sesudo` runs, it returns one of the following values.

- **-2**  
Target user is not found, or command interrupted
- **-1**  
Password error
- **0**  
Execution successful
- **10**  
Problem with usage of parameters
- **11**  
syscall is not loaded
- **20**

- Target user error
- **22**  
syscall is loaded but the daemon is not running
- **30**  
Authorization error

This command has the following format:

```
sesudo {-h|-list|record [params]}
```

- **-h**  
Displays the help screen
- **-list**  
Lists sesudo commands that you can execute. These are the SUDO records defined in the Privileged Access Manager database that you are authorized to execute.
- **record**  
Specifies the name of the SUDO class record the security administrator gave to the command you want to execute using the sesudo utility
- **params**  
(Optional) Specifies the parameters that you want to send to the command you are executing

## sesudo Utility Execute a Command as Another User on Windows

### Valid on Windows

The sesudo utility executes commands for one user with the permissions of another user. The sesudo utility borrows the permissions of another user (the *target* user) to perform one or more commands. The utility allows regular users to perform actions such as the mount command, which requires superuser authority.

The rules governing user authority to perform commands in this way are defined as access rules in the SUDO class. A record in the SUDO class contains a command script, and can specify both users who are permitted to run the script with sesudo and forbidden users.

**Note:** The user executing the program that is invoked by sesudo cannot be changed from Privileged Access Manager for Windows.

This command has the following format:

```
sesudo {-h|-list|-do record [params]}
```

- **-h**  
Displays the online help screen
- **-list**  
Lists sesudo commands that you can execute. Lists the SUDO records that are defined in the product database that you are authorized to execute.
- **-do record [params]**  
Specifies that sesudo executes a command as another user
  - **record**  
Specifies the name of the SUDO class record the security administrator gave to the command that you want to execute using the sesudo utility
  - **params**  
(Optional) Specifies the parameters that you want to send to the command that you are executing

## seuidpgm Utility - Extract Trusted Programs

### Valid on UNIX

The seuidpgm utility extracts all the programs whose Set-User-ID bit or Set-Group-ID bits are on. seuidpgm traverses a file system and creates the selang commands for adding these programs to the PROGRAM class.

seuidpgm creates the commands in the selang command language and writes them to the standard output. You can use a pipeline to the selang utility, or redirect the output to a file. We recommended that you redirect the output to a file, because then you can edit the output to remove unwanted programs or add additional programs. Use this procedure to search for undesirable setuid programs in your system.

#### NOTE

We recommended that you run the UxImport utility to define users and groups before running the seuidpgm utility. However, if you have not run UxImport, you can use seuidpgm with the -g and -u options to define users and groups.

seuidpgm descends through the paths specified at the command line to all subdirectories of the starting path. Multiple start paths are allowed.

You can specify any number of options. When specifying more than one option, separate the options with spaces.

If a program is a setuid program and has write access, seuidpgm treats the program like all other setuid programs, but also sends a warning to standard error.

#### NOTE

For more information about how to control PROGRAM class records, see [Endpoint Administration Guide for UNIX](#).

This command has the following format:

```
seuidpgm optionstartDir ... [-x excludeDir]
```

- **-d**  
Automatically creates entries for setuid and setgid programs in the PROGRAM class, with defaccess set to execute, instead of analyzing the file permissions in UNIX to determine the permitted file access. In some cases, one setuid or setgid program executes another one. If you do not include this option, the program trying to execute the setuid or setgid program is *not* able to execute it.  
We recommend that you use this option.
- **-f**  
Creates rules for both the FILE and PROGRAM classes.
- **-g**  
Creates GROUP records for setgid programs.

#### NOTE

Use this option *only* if you have *not* run UxImport.

- **-l**  
Creates a single permit for programs which have *hard* or *symbolic* links.  
If you want to scan your file system from some directories only (not from the root directory) and to include the -l option, use multiple starting paths on the command line; otherwise the -l option might be inefficient.
- **-n**  
Does not traverse NFS at all.  
We recommend that you use this option.
- **-o**  
Writes the file names to the standard output but does not create selang commands.
- **-p**

Enables setuid programs from NFS directories, but only when the mount table allows setuid from that mounted file system.

- **-q**  
Runs the utility in Quiet-Mode; error messages are not sent to standard error.
- **-s**  
Creates entries for setuid/setgid programs in class SECFILE, instead of creating entries for the PROGRAM class.
- **-u**  
Creates USER records for setuid programs.

#### NOTE

Use this option *only* if you have *not* run UxImport.

- **-x *excludeDir***  
Excludes a directory from the tree. The specified directory is not searched for setuid and setgid programs. This option must be the last option specified in the command line. *Path* is the full path of the directory to be excluded. To exclude more than one directory, repeat the -x option for each directory.
- ***startDir***  
Specifies a space-separated list of top directories to search for trusted programs.

### Examples

- The following command prints selang commands to add all programs with set-user-id or set-group-id turned on, defaccess execute, checking for duplicate names or the same inode, in quiet mode, and without passing through NFS. The program scans from the /usr directory and its subdirectories, the /var directory and its subdirectories, and the /etc directory and its subdirectories. Output is directed to the file seprogs.seos in your home directory.

```
seuidpgm -dlqn /usr /var /etc > ~/seprogs.seos
```

The output looks similar to the following code:

```
## *****
```

```
## seuidpgm List Sun Feb 9 14:24:16 1997
```

```
# Start Path= /usr
```

```
# *****
```

```
nr PROGRAM /usr/lpp/bos/inst_root/lpp/inu_LOCK defaccess(EXEC) nr PROGRAM /usr/lpp/X11/bin/xlock
defaccess(EXEC) nr PROGRAM /usr/bin/setenv defaccess(EXEC) nr PROGRAM /usr/bin/shell defaccess(EXEC) nr
PROGRAM /usr/bin/su defaccess(EXEC) nr PROGRAM /usr/bin/sysck defaccess(EXEC) nr PROGRAM /usr/bin/tcbck
defaccess(EXEC) nr PROGRAM /usr/bin/usrck defaccess(EXEC) nr PROGRAM /usr/bin/vmstat defaccess(EXEC)
```

- The following command scans the root directory and all its subdirectories, except the /home directory:

```
seuidpgm -qln / -x /home
```

## seversion Utility Display CA Privileged Access Manager Server Control Program Module Version Information

### Valid on UNIX

The seversion utility displays information regarding the version of a Privileged Access Manager module. You can display the following data:

- The global and minor version numbers
- The date and time that the module was compiled
- The station that the module was compiled on
- SHA signatures

This command has the following format:

```
seversion [-a|-l|-g|-h|-m|-s|-s256|-s384|-s512|-5] module
```



- **-a**  
Displays the requested information in table format
- **-g**  
Displays only the global version number, without titles
- **-h**  
Displays the help for this utility
- **-l**  
Displays included library information
- **-m**  
Displays only the minor version number, without titles
- **-s**  
Displays the SHA1 signature, without titles
- **-5**  
Displays the MD5 signature, omitting titles.  
This option works only while not in FIPS-only mode.
- **-s256**  
Displays the SHA256 signature, without titles
- **-s384**  
Displays the SHA384 signature, without titles
- **-s512**  
Displays the SHA512 signature, without titles
- *module*  
Specifies the file name of the module whose version number you want to display

### Example

To display version information for the `sesudo` utility, enter the following command:

```
seversion /opt/CA/PAMSC/bin/seosd
```

A message similar to the following appears on the screen while not in FIPS mode:

```
CA ControlMinder seversion vX.X.X.xxx - Display module's version

Copyright (c) YYYY CA. All rights reserved.

Running under:  Linux

File name: /opt/CA/PAMSC/bin/seosd

Version   : major.minor.sp.build

Created   : MMMDDYYYYhh:mm:ss

OS info   : i86PC

SHA1      : 10068CC6A70195B84AF896682CCBA1A4B7B43CD1
```

MD5: : 1F9BD56CA523A33FFBC47551ECE093E5

## sewhoami Utility Display Your PAM SC Server Control User name and Security Credentials on UNIX

### Valid on UNIX

The sewhoami utility displays the user name as it is known to the Privileged Access Manager authorization daemon. sewhoami is similar to the whoami utility provided by UNIX systems, but it produces different and often more useful information:

- If the user executes an su command and then executes the UNIX whoami utility, it displays the user name according to the user ID acquired after executing the su command.
- If the user executes an su command and then executes the Privileged Access Manager sewhoami utility, it displays the original login ID of the user; it also displays authorization information.

This command has the following format:

```
sewhoami [-a|-d]
```

- **-a**  
Displays the user credentials; that is, the contents of the user ACEE

#### NOTE

For more information about the ACEE, see the *Endpoint Administration Guide for UNIX*.

- **-d**  
Displays the ACEE handle that is associated with the user and the handle name in the database

### Example: Display Your Privileged Access Manager User Name and Security Credentials on UNIX

This example displays your own user name and security credentials as they are known to the Privileged Access Manager authorization daemon:

```
sewhoami -a
```

If you are a root user, the sewhoami output might look like the following example:

```
root
ACEE Contents
User's Name : root
ACEE's Handle : 52
Group Connections Table:
Group Name Connection Mode
=====
admRegular
bin Regular
daemon Regular
disk Regular
root Regular
seosaudt Regular
sys Regular
wheelRegular
Categories : <None>
Profile Group : <None>
Security Label : <None>
User's Audit Mode : Failure LoginSuccess LoginFailure
```

```

User's Security Level : 0
Source Terminal : <Unknown>
Process Count for ACEE : 19
User's Mode : Admin Auditor
ACEE's Creation Time : Tue Mar 17 14:53:07 2009

```

If you are a user who is named test, not a root user, then the sewhoami output might look like the following example:

```

test
ACEE Contents
  User's Name : test
  ACEE's Handle : 65
  Group Connections Table:
  Group Name Connection Mode
  =====
  seosaudt Regular
  users Regular
Categories : <None>
Profile Group: secadmin
Security Label : <None>
User's Audit Mode : Failure LoginSuccess LoginFailure
User's Security Level : 0
Source Terminal : localhost.localdomain
Process Count for ACEE : 2
User's Mode : Admin Auditor
ACEE's Creation Time : Wed Mar 18 15:34:53 2009

```

## uninstall\_AC Utility Remove CA Privileged Access Manager Server Control from the Current Computer

### Valid on UNIX

The `uninstall_AC` utility removes all or part of Privileged Access Manager from the station on which you execute the command. The default (`-all`) removes the entire product from the station.

#### NOTE

Unload the Privileged Access Manager kernel extension before uninstalling.

This command has the following syntax:

```
uninstall_AC [-all | -admin] [-f] [-force] [-h] [-ignore_dep] [-d path] [-fn file]
```

- **-admin**

Removes only administration tools such as Security Administrator and seauditx from the station

#### NOTE

The *admin* package is no longer included with Privileged Access Manager. This option is used for removing older versions of Privileged Access Manager.

- **-all**

Removes the entire product from the station

- **-d path**

Defines the directory where Privileged Access Manager is installed

**NOTE**

If Privileged Access Manager is installed in the default directory (/opt/CA/PAMSC), you do not need to specify this option.

- **-f**  
Removes Privileged Access Manager in silent mode
- **-fn *file***  
Executes the specified file after the uninstall completes
- **-force**  
Forces uninstall to proceed even if the kernel extension unload process fails
- **-h**  
Displays the help for this utility
- **-ignore\_dep**  
Specifies that the uninstallation procedure does not verify dependency with other products

**Example: Completely remove Privileged Access Manager from a computer**

To remove Privileged Access Manager from this computer completely, if it was installed in the default directory, enter the command:

```
uninstall_AC
```

**uxauthd.sh Script Administer UNIX Authentication Broker Agent**

Use the uxauthd.sh script to administer the UNIX Authentication Broker agent. We recommend that you use the uxauthd.sh script to administer the UNIX Authentication Broker agent. This helps ensure that the environment is configured correctly.

The uxauthd.sh script is located in the following directory, by default: /opt/CA/uxauthd/sbin.

This command has the following format:

```
uxauthd.sh {start | stop | restart | status | debug level}
```

- **start**  
Starts the UNIX Authentication Broker agent
- **stop**  
Stops the UNIX Authentication Broker agent
- **restart**  
Restarts the UNIX Authentication Broker agent
- **status**  
Displays the status of the UNIX Authentication Broker agent. The status states are:
  - uxauthd running
  - uxauthd not running
- **debug *level***  
Specifies to start the UNIX Authentication Broker agent in debug level  
**Range:** 1-3

**NOTE**

Using uxauthd.sh to start or stop the UNIX Authentication Broker agent affects the status of the Report Agent.

## uxauth\_selinux.sh Enable SELinux Support

The `uxauth_selinux.sh` script deploys a SELinux policy that enables UNIX Authentication Broker to work in SELinux environment. The script enables support for the following utilities: `ssh`, `rlogin`, `ftp`, `sftp`, and `passwd`.

You can install the SELinux UNIX Authentication Broker policy using the extensive or the general installations. Extensive installation adds permissions for the SELinux security context type `usr_t`. General installation does not add permissions for the `user_t` type and hence UNIX Authentication Broker cannot support offline users login and user login reports.

The `uxauth_selinux.sh` script is located in the *UNIX Authentication Broker lbin* directory, by default: `/opt/CA/uxauthd/lbin`. The `uxauth` installation package can be customized to run the script during UNIX Authentication Broker installation where SELinux policy is installed in general mode. You can also run the script after installation from the default location.

### NOTE

Installing an extensive policy automatically uninstalls previously installed general policy.

This command has the following format:

```
uxauth_selinux.sh {-i [-e] | -r | -h}
```

- **-i**  
Installs the policy in the SELinux environment
- **-e**  
Specifies to invoke the extensive installation option that adds permissions for the `usr_t` type
- **-r**  
Removes the policy from the SELinux environment
- **-h**  
Displays the help

## uxconsole Utility Manage UNIX Authentication Broker Endpoints

The `uxconsole` utility lets you manage your UNIX Authentication Broker endpoints. Use the `uxconsole` utility to complete the following tasks:

- Display information about the UNIX Authentication Broker installation
- Register the UNIX Authentication Broker endpoint in Active Directory
- Manage and migrate users and groups.

The utility handles several tasks and has the following functions:

Task	Function
Register UNIX computers in Active Directory	<a href="#">uxconsole -register</a>
Deregister UNIX computers in Active Directory	<code>uxconsole -deregister</code>
Set verbosity level	<a href="#">uxconsole -debug</a>
Activate login for Active Directory users	<code>uxconsole -activate</code>
Deactivate login for Active Directory users	<code>uxconsole -deactivate</code>
Manage users mapping	<a href="#">uxconsole -map</a>
Migrate users and groups to Active Directory	<a href="#">uxconsole -migrate</a>
Manage users and groups	<a href="#">uxconsole -manage</a>
Display endpoint status	<a href="#">uxconsole -status</a>
Perform Kerberos operations	<a href="#">uxconsole -krb</a>
Perform LDAP queries in Active Directory	<a href="#">uxconsole -ldap</a>

Display UNAB NSS cache data	<a href="#">uxconsole -db -dump</a>
Delete Active Directory Users and Groups	<a href="#">uxconsole -db -del</a>
Verify Active Directory user accounts	<a href="#">uxconsole -verify</a>
Takes a snapshot (static mode) of the current AD topology (Domains, DCs, DNS, and so on) and saves in the Kerberos configuration section of the uxauth.ini file. To switch back to the default mode (dynamic mode), re-register (deregister and register again) UNAB. You can also manually update the Kerberos configuration section in the <a href="#">uxauth.ini</a> file.	<a href="#">uxconsole -freeze</a>

## uxconsole -map Manage Users Mapping

### Valid on UNIX

Use the map command to NIS or local user accounts to Active Directory user accounts.

#### NOTE

When you use the -map option, the uxconsole utility does not connect to Active Directory to identity conflicts in user account details.

This command has the following formats:

```
uxconsole -map [-add] [-scope {l|n|a}] { -all | <unix_name> [ <ad_name>] | -input <file> } [-d <domain> ] [-force] [-v]
uxconsole -map -local { <unix_name> | -input <file> } [-force] [-v]
uxconsole -map -del { <unix_name> | -input <file> } [-force] [-v]
uxconsole -map -show [<filter>] [-scope {l|n|a}] [-v]
uxconsole -map -h
```

- **-add**  
Add users mapping
- **-scope {l|n|a}**  
Specifies the mapping scope:
  - lmap the local user accounts only
  - nmap NIS/NIS+ user accounts only
  - amap local and NIS/NIS+ user accounts
- **-all**  
Specifies to map all NIS and or local user accounts with identical user names
- **<unix name>**  
Specifies to map a single UNIX user account, either NIS or local account

#### NOTE

You can also use this parameter to delete mapped NIS or local user accounts.

- **-ad <ad name>**  
Specifies the Active Directory name of the local user account
- **-input <file>**  
Specifies an input file containing mapping requests. Create the map file in a CSV format with the following fields and parameters:  

```
<unix_name>,[<ad_name>],[<domain>]
```
- **<unix\_name>**  
Specifies the UNIX user account name
- **[<ad\_name>]**

Specifies the Active Directory user account. *ad\_name* is an optional parameter. If you do not specify the Active Directory user account, the account is mapped to an AD account with the same UNIX user account name.

- **[<domain>]**  
Specifies the domain name of the Active Directory account. *domain* is an optional parameter
- **-d <domain>**  
Defines the Active Directory domain name that contains the user account

**NOTE**

You can specify the full user credentials using the following format: *<name>@<domain>*. If the domain name is not specified, then the domain is mapped to the registration domain.

- **-force**  
Specifies to force user mapping and overwrite existing mapping or migration status or delete user mapping

**NOTE**

By default, uxconsole does not delete partially migrated user accounts.

- **-local**  
Specifies to set the user account as a local exception

**NOTE**

If you specify a user as local exception, UNIX Authentication Broker does not manage the user account, although an identical user account may exist in the Active Directory.

- **-del**  
Specifies to delete local or NIS user mapping
- **-show**  
Specifies to display users mapping details

**<filter>**

Defines the wildcard that returns a subset of users

- **-v**  
Specifies to activate verbosity
- **-h**  
Displays the help

## uxconsole -manage Manage Users and Groups

### Valid on UNIX

Use this command to list or information for local or enterprise users and groups.

This command has the following formats:

```
uxconsole -manage {-find | -show [-detail]} {-user <filter> | -group <filter>}
```

```
uxconsole -manage -show -policy
```

- **-find**  
Specifies to display a list of local and enterprise users or groups
- **-show**  
Specifies to show the details of a specific user or group, a subset of users and groups, or to show policies
- **-detail**  
Specifies to display the user settings in detail
- **-user *filter***

Defines the wildcard that returns a subset of users

- **-group *filter***  
Defines the wildcard that returns a subset of groups
- **-policy**  
Specifies to display the enterprise login policy

### Example: Display User Status

The following example shows you the output for a local UNIX user (local1) who is mapped to an Active Directory user with a different name (ent1). The Active Directory user has UNIX attributes enabled, so can log in to the UNIX Authentication Broker endpoint:

```
uxconsole> ./uxconsole -manage -show -detail -user ent1
```

```
CA PAMSC UNAB uxconsole v12.52.0.160 - console utility
```

```
Copyright (c) YYYY CA. All rights reserved.
```

```
USER 'ent1' information
```

```
-----
```

```
Type                : Local User
```

```
Login Name          : local1
```

```
Mapped to           : ent1@example.com
```

```
Enterprise Account   : Enabled
```

```
Local Account        : Enabled
```

```
Login               : Allowed
```

```
Login Reason         : User exists locally
```

```
Uid                  : 300
```

```
Gid                   : 101
```

```
Shell                 : /bin/bash
```

```
Home Directory        : /home/local1
```

```
Unix Groups           : 30017(unabca_gx2), 30016(unabca_gx1) All Groups           : unabca_gw1@comp
```

```
Type                : Enterprise User
```



```

Login Name           : ent1
Principal Name       : ent1@example.com
Enterprise Account    : Enabled
Login                : Allowed
Login Reason          : According to internal default
Uid                  : 10133
Gid                   : 13870
Shell                 : /bin/sh
Home Directory        : /home/ent1

```

## uxconsole -migrate Migrate UNIX Users and Groups to Active Directory

### Valid on UNIX

Using the migrate command migrates users and groups from the UNIX host into Active Directory. The migration process attempts to migrate local users and groups into Active Directory and disable the local accounts.

This command has the following format:

```

uxconsole -migrate [-scope {l|n|a}] {-mode {p|f}}[-input file] [-emulate] [-d domain] [-a name [-w pass]] [-
users] [-groups] [-cgc container] [-new] [-v level] [-h]
uxconsole -migrate [-show {-user filter|-group filter}]

```

- **-migrate**  
Defines the UNIX users migration option.
- **-scope {l | n | a}**  
Specifies the migration scope:
  - l migrate only local users and groups.
  - n migrate NIS users and groups from NIS/NIS+ server.
  - a migrate local and NIS/NIS+ users and groups.**Default:** l
- **-mode {p | f}**  
Specifies the migration mode.  
**Options:** partial, full  
**Default:** f
- **-input file**  
Defines the full path of the accounts map file.

### NOTE

Use the mapping file to resolve conflicts in user accounts that were discovered during the migration process. Create the map file in a CSV format with the following fields and parameters:

```
type <USER|GROUP>, UNIX name <username>, requested action <KEEPLocal|MIGRATE|MAP>, AD name <AD mapped name>
```

**Example:** USER,uxuser, MAP,aduser.

**WARNING**

You cannot specify the GROUP type to use the MAP action. You can use the MAP option to map user accounts only.

- **-emulate**

Specifies that the migration process runs in emulation mode.

**NOTE**

Running the uxconsole -migrate command in emulation mode does not migrate users to Active Directory. In emulation mode the uxconsole creates a journal file that reports on possible conflicts in users and groups IDs. Use the emulation mode to resolve conflicts between UNIX and Active Directory users and groups IDs.

- **-d *domain***

Defines the name of the domain to migrate users and groups to.

**NOTE**

Running the -migrate -d command without supplying the administrator credentials does not enable UNIX Authentication Broker to migrate users and groups to Active Directory.

- **-a *name***

Specifies the Active Directory administrator used to register, create, and update users properties in Active Directory.

**Note:** Running the -migrate command without supplying the administrator credentials does not enable UNIX Authentication Broker to append UNIX attributes nor to add accounts or groups to Active Directory. You cannot resolve conflicts that were discovered during migration without supplying the Active Directory administrator credentials.

- **-w *passwd***

Specifies the Active Directory administrator's account password.

- **-users**

(Optional) Specifies that only users are migrated to Active Directory.

**NOTE**

If not specified, all the users are migrated to Active Directory.

- **-groups**

(Optional) Specifies that only groups are migrated to Active Directory.

**NOTE**

If not specified, all the groups are migrated to Active Directory.

- **-cgc *container***

Specifies the name of the Active Directory container where new groups are created.

- **-new**

Specifies to migrate only new users and groups that were not previously migrated.

- **-v *level***

Specifies the verbose level.

**Range:** 1-5

- **-h**

Displays the help.

- **-show**

Displays users and groups migration information.

**NOTE**

If specified, users and groups are not migrated.

- **-user *filter***

Displays only those users that match the filter criteria.

- **-group *filter***

Displays only those groups that match the filter criteria.

## uxconsole -register Register UNIX Computers in Active Directory

### Valid on UNIX

Use the *uxconsole* command to register a UNIX host in Active Directory. A privileged account (not necessarily administrator account) user can register a UNIX host in Active Directory. To let the Active Directory users log in to the UNIX host, activate the UNIX Authentication Broker.

You can run the command multiple times on the same computer.

Example: Run the command to repair the UNIX Authentication Broker host registration with Active Directory when the keytab file is deleted.

The *uxconsole* command has the following format:

```
uxconsole -register -a name [-w pass] [-d domain] [-t site] [-v level] [-n] [-o container] [-s server] [-p #]
  [-sso] [-i #] [-h] [-k]
uxconsole -register -owt -d domain -a name [-w pass] [-v level]
uxconsole -register -owt -pupm -d domain -a name -epname name [-eptype type] [-container name] [-v level]
uxconsole -deregister -owt -d domain [-a name] [-v level]
uxconsole -deregister -a name [-w pass] [-d domain] [-v level] [-o container] [-s server] [-p #]
```

- **-register**  
Specifies that Active Directory registers UNIX Authentication Broker.
- **-deregister**  
Specifies that Active Directory deregisters UNIX Authentication Broker.
- **-a name**  
Specifies a user with privileges to register computers in Active Directory.  
**Default:** administrator
- **-epname**  
Specifies an endpoint where the privileged account originates.
- **-eptype**  
Specifies the endpoint type. If not otherwise specified, the endpoint type is Windows Agentless.
- **-w pass**  
Specifies the password of a user with privileges to register computers in Active Directory.
- **-d**  
Defines the domain name that the Active Directory is part of.
- **-h**  
Displays the program help.
- **-n**  
Specifies that the uxauthd agent runs after the registration process completes.
- **-o container**  
Specifies the Active Directory container name where you register the UNIX computer. The Active Directory container must exist before you register the UNIX computer.
- **-container**  
Specifies the name of the container where you register the privileged account.
- **-owt**  
Specifies a position-dependent argument that requests the proxy user key management. Register the UNIX Authentication Broker endpoint before using this option.
- **-p #**  
Specifies the Active Directory listening port number.
- **-pupm**  
Specifies to use Shared Account Management integration.
- **-s server**

Specifies the Active Directory Server name.

- **-sso**  
Specifies that the uxconsole manages Kerberos files for Single Sign On (SSO)
- **-t site**  
Defines the Active Directory site that contains Domain Controllers (DCs). The UNIX Authentication Broker uses DCs to communicate with the Active Directory. The UNIX authentication broker writes the site name to the `ad_site` configuration setting in the `ad` section of the `uxauth.ini` file. We recommend that you do not specify this option. If you do not specify this option, the utility automatically selects the best Active Directory site to use.

#### NOTE

The values in the `ignore_dc_list` and `lookup_dc_list` configuration settings affect how UNIX Authentication Broker implements Active Directory site support.

- **-v level**  
Defines the verbose level to use during the installation process.
- **-i #** Specifies the Key Distribution Server (KDC) configuration mode. **Limits:** 0 - Use host name for the registered domain KDC in Kerberos configuration  
1 - Use IP address instead of hostnames for KDC in Kerberos configuration  
2 - Use DNS-only KDC lookup  
**Default:** 0
- **-k** Specifies to skip the key version when the Active Directory fails to increase the key version on the Kerberos token.

### Example: Register a UNIX Host in Active Directory

The example shows how to register a UNIX computer in Active Directory by providing the following information:

- User name (-a administrator)
- Password (-w admin)
- Set the verbosity level (-v 3)
- Specify that the UNIX Authentication Broker agent does not run at the end of the installation (-n)
- Define the name of the container in Active Directory (-o OU=COMPUTERS), where the computer object representing the endpoint locates. The container must exist before you register the UNIX computer in Active Directory:

```
./uxconsole -register -a administrator -w admin -v 3 -n -o OU=COMPUTERS
```

For assistance while registering the UNIX host on Active Directory, refer to the following topics:

- [uxconsole -krb Perform Kerberos Operations](#)
- [uxconsole -ldap Perform LDAP queries in Active Directory](#)

### uxconsole -status Display UNIX Authentication Broker Status

#### Valid on UNIX

Use this command to display the status of UNIX Authentication Broker on the endpoint. Using the `-detail` argument displays all the available information about the status of UNIX Authentication Broker.

This command has the following format:

```
uxconsole -status [-detail]
```

- **-status**  
Specifies to display the UNIX Authentication Broker status.
- **-detail**

Specifies to display the UNIX Authentication Broker status in detail.

**Example: Display the UNIX Authentication Broker Status in Detail.**

The following example shows you the output that you receive when you run the `uxconsole - status -detail` command.

```
#./uxconsole -status -detail

CA PAMSC uxconsole v12.52.0.160 - console utility

Copyright (c) YYYY CA. All rights reserved.

Registration domain - example.com

DCs                - computer1, computer2

User search base    - DC=unixauth,DC=example,DC=com

User search filters

    Include         - CN=Users; OU=Test

    Exclude         - OU=WrongOU

Group search base    - CN=Users,DC=example,DC=com

Group search filters

    Exclude         - OU=Computers

Trusted domain      - DC=unab,DC=example,DC=com

DCs                - winserver

User search base     - DC=unabdom,dc=example,dc=com

User search filters

    Include         - CN=users

Group search base     - DC=unab,DC=example,DC=com

UNAB mode - full integration

UNAB status - activated

Agent status - running, pid = 6178
```

---

```
SELinux status          - permissive

SELinux UNAB policy     - uxauth_ex  (version: 1.0)

CA AC server host       - ssl://acserver.example.com:7243

CA AC server status     - connected (updated: Wed Jun 27 18:11:36 YYYY)

Time sync- enabled (NTP server: 192.168.1.10.0 or fd6d:8d64:af0c:1:0:242:22:233)

Enterprise policy - login@computer.com (updated: Wed Jun 27 18:11:36 YYYY)

Enterprise policy - loginHG@GHNODE#01 (updated: Wed Jun 27 18:11:36 YYYY)

Local policy - enabled

Default login access - deny

AD Unix users - 16 (updated: Wed Jun 27 18:11:36 YYYY)

AD Unix groups - 8 (updated: Wed Jun 27 18:11:36 YYYY)

AD Windows groups - 19 (updated: Wed Jun 27 18:11:36 YYYY)

Migration - not migrated

CA PAMSC - installed

  Include AD users and groups in AC ladb : yes

  Display AD names in AC Audit : no

  Support AD non-Unix groups in AC: yes

  PAM authentication in AC utilities : yes
```

In this example, the output displays the following information:

- The Active Directory domain name - example.com
- The DCs with which the endpoint communicates - computer1, computer2
- The user and group search base filters
- The trusted domain - unab.example.com
- UNAB mode - full integration
- UNAB status - activated
- UNAB agent (uxauthd) status - running, pid = 6178
- The SELinux installation status - permissive
- The deployed SELinux UNAB policy - uxauth\_ex (version: 1.0)
- The CA AC server host name or IP address
- The CA AC server connection status
- Whether time synchronization was activated - enabled
- The NTP server IP address - 192.168.1.100 (IPv4) or fd6d:8d64:af0c:1:0:242:22:233 (IPv6)
- The name of deployed enterprise login policies - login@computer.com, loginHG@GHNODE#01
- When the enterprise login policies were last updated
- Whether local login policy is activated - enabled
- Whether the default login policy is enabled - deny
- The number of UNIX users in Active Directory - 16 and the time that they were last updated
- The number of UNIX groups in Active Directory - 8 and the time that they were last updated
- The number of Windows groups in Active Directory - 19
- The time that the UNIX users and groups and Windows groups were last updated
- The migration status of the users - not migrated
- Whether Privileged Access Manager is installed on this endpoint - installed
- Whether to include information regarding Active Directory users and groups in the Privileged Access Manager ladb - yes
- Whether to display Active Directory users and groups names in Privileged Access Manager audit records - yes
- Whether Privileged Access Manager supports non-UNIX Active Directory groups - yes
- Whether to support PAM authentication in Privileged Access Manager utilities - yes

## uxconsole -krb Perform Kerberos Operations

### Valid on UNIX

Use this command to perform Kerberos operations from the UNIX Authentication Broker endpoint. For example, creating tickets. You do not need to install Kerberos on the endpoint to perform Kerberos operations.

This command has the following format:

```
uxconsole -krb [-init | -list | -passwd | -vno | -destroy | -resolve]
```

- **-init**  
Specifies to obtain and cache a ticket.
- **-list**  
Displays the content of a credentials cache or keytab.
- **-passwd**  
Specifies that an Active Directory user can modify password directly in the Active Directory on the end point using Kerberos protocol. To change the password, UNAB need not run on the endpoint. The passwd command also allows

a user with sufficient Active Directory privileges to reset password of another user. That is, a user performs an administrative change without the need to do it on Windows.

```
uxconsole -krb -passwd [-i kcf] [-h] [principal]
```

```
uxconsole -krb -passwd -a admin [-i kcf] principal
```

- **-i kcf**  
Specifies that the Kerberos configuration is used from a file named "kcf".
- **-h**  
Specifies the help screen.
- **-a**  
Specifies that an admin authenticates to the Active Directory as admin and changes the password for a principal.  
**Note:** An account admin must have appropriate privileges in the Active Directory.
- **principal**  
Specifies the principal that is known to the Active Directory. A principal name is required when the user is not located in the registration domain.
- **-vno**  
Displays the key version number for Kerberos principals.
- **-destroy**  
Specifies to destroy the credentials cache.
- **-resolve**  
Specifies to resolve a host name or IP address.

#### Example: Obtain a Ticket Granting Ticket (TGT) using UNIX Authentication Broker keytab

The following example shows how you obtain a TGT using UNIX Authentication Broker keytab:

```
./uxconsole -krb -init -k
```

#### Example: List the content of the credentials cache

The following example shows how you list the content of the credentials cache:

```
./uxconsole -krb -list
```

#### Example: List the content of the keytab with encryption data

The following example shows how to display the content of the keytab including available encryption information:

```
./uxconsole -krb -list -keytab
```

### uxconsole -ldap Perform LDAP queries in Active Directory

#### Valid on UNIX

Use this command to perform LDAP queries on Active Directory from a UNIX Authentication Broker endpoint that does not have LDAP installed. Use this command instead of the ldapsearch utility. You can use this command to troubleshoot UNIX Authentication Broker installation. For example, you can query Active Directory for the container to use.



**WARNING**

Verify that you have a Ticket Granting Ticket (TGT) before you use this command. You can obtain a TGT using the command: `uxconsole -krb`.

**NOTE**

The LDAP filter must comply with "RFC 2254".

This command has the following format:

```
uxconsole -ldap -search -delete [-d DC] [-p port] [-b base] [-s scope] [filter [attributes]]
```

- **-search**  
Specifies the search option
- **-delete**Deletes a user from the Active Directory.
- **-d *DC***  
Specifies the Domain Controller to query
- **-p *port***  
Specifies the LDAP port to use
- **-b *base***  
Specifies the search base
- **-s *scope***  
Specifies the search scope  
**Default:** sub
- **filter [*attributes*]**  
Specifies the filter and attributes to use

**NOTE**

If you do not specify a filter, the '(objectClass=\*)' is used. If you do not specify any attributes, the select all option ('\*') is used.

**Example: Display a DSE**

The following examples shows how you display a DSE:

```
./uxconsole -ldap -search '(&(objectClass=user) (objectCategory=user) )'
```

**uxconsole -dbdump Display UNAB NSS cache data****Valid on UNIX**

Use this command to display users and groups information from the UNIX Authentication Broker NSS database. You can use this command to view information about users and groups that are defined in Active Directory.

This command has the following format:

```
uxconsole -db -dump [-a] table [item]
```

- **-a**  
Displays extension fields.
- **table [*item*]**  
Displays the content of the specified table and items.

**NOTE**

If you do not specify the table name, this command displays all the supported tables. The supported tables are: pw (table with user attributes); gr (table with group attributes)

**Example: Display all Active Directory users stored in cache**

The following example shows how to display all Active Directory users who are stored in the endpoint cache:

```
./uxconsole -db -dump pw
```

#### **Example: Display all Active Directory groups stored in cache**

The following example shows how to display all Active Directory groups that are stored in the endpoint cache:

```
./uxconsole -db -dump gr
```

### **uxconsole -db -del Delete Active Directory Users and Groups**

#### **Valid on UNIX**

Use this command to delete users and groups from the Active Directory.

This command has the following format:

```
uxconsole -db -del table item
```

- **table** [*item*]  
Deletes the content of the specified table and items.

#### **NOTE**

If you do not specify the table name, this command displays all the supported tables. The supported tables are: pw (table with user attributes); gr (table with group attributes)

#### **Example: Delete all Active Directory users stored in cache**

The following example shows how to delete all Active Directory users who are stored in the endpoint cache:

```
./uxconsole -db -del pw
```

#### **Example: Delete all Active Directory groups stored in cache**

The following example shows how to delete all Active Directory groups that are stored in the endpoint cache:

```
./uxconsole -db -del gr
```

### **uxconsole -debug Set Verbosity Level for Modules**

#### **Valid on UNIX**

Use this command to set the verbosity level per module. UNIX Authentication Broker also sends PAM and NSS debug information to log files.

This command has the following format:

```
uxconsole -debug -m mod [-v level]
```

- **-m** *mod*  
Specifies the module to set the verbosity level  
**Options:** nss, pam, agent, all
- **-v** *level*  
Specifies the verbosity level.  
**Limits:** 0-5

UNIX Authentication Broker writes the debug information to the following files:

```
UNABInstallDir/log/debug/pam_debug
UNABInstallDir/log/debug/pam_debug.back
```

```
UNABInstallDir/log/debug/nss_debug
UNABInstallDir/log/debug/nss_debug.back
```

**NOTE**

If you set the verbosity level to more than 0 while the agent is not running, you receive a message indicating that the UNIX Authentication Broker PAM module was activated. UNIX Authentication Broker sends the debug information to the syslog only.

**uxconsole -verify Verify Active Directory User Account UNIX Attributes****Valid on UNIX**

Use this command to verify that an Active Directory user account is ready for use by UNIX Authentication Broker. This command locates the user account and verifies that the UNIX attributes (login shell, home directory, UID and GID) are consistent with the values as they exist in the UNIX Authentication Broker user cache database.

**NOTE**

This command does not verify the user password.

This command has the following format:

```
uxconsole -verify -user <user_name>[<user_name1>][<user_name2>...]
```

- **-user**  
Specifies to verify the user account UNIX attributes in Active Directory
- **<user\_name>**  
Specifies the Active Directory user account.

**Example: Verify Active Directory user account UNIX attributes**

The following example shows how to verify Active Directory user account UNIX attributes:

```
./uxconsole -verify -user Joe
```

In this example, you use the -verify command to verify the user account Joe UNIX attributes. UNIX Authentication Broker does the following:

- Checks the /etc/shells file to verify that the login shell specified is supported
- Verifies that the user name length consists with the limitations as imposed by the operating system
- Verifies that the home directory is specified
- Verifies that the UID is specified
- Verifies that the GID is specified

**How uxconsole Discovers an Active Directory Site**

When you register a UNIX Authentication Broker endpoint with Active Directory, by default the uxconsole utility discovers the closest Active Directory site and communicates only with domain controllers (DCs) in this site.

The following process describes how uxconsole discovers the closest Active Directory site:

1. The UNIX Authentication Broker endpoint queries the DNS for SRV (service) records in the following format:  
\_ldap.\_tcp.dc.\_msdcs.*domainName*  
The DNS returns the records for DCs in the domain.
2. The endpoint accesses Active Directory by binding and authenticating to a DC returned in the previous query.

**NOTE**

The endpoint can bind to any of the returned DCs.

3. The endpoint uses an LDAP query to search Active Directory for the site in which the endpoint resides. The query uses the following filters:
  - Base Dnno value
  - ScopeBase
  - AttributeNetlogon
  - DnsDomainFully-qualified domain name
  - ntver6.00
 For example, Filter on (&(DnsDomain=example.company.com)(ntver=6.00))  
 The DC returns the name of the site in which the endpoint resides.  
**Note:** The DC uses the endpoint IP address to determine the site in which the endpoint resides.
4. The endpoint queries the DNS for SRV records in the following format:  
`_ldap._tcp.Local/SiteName._sites.dc._msdcs.domainName.`  
 The DNS returns the records for DCs in the site in which the endpoint resides. The endpoint communicates only with DCs in this site.

## UxImport Utility Extract Information from the UNIX Operating System

### Valid on UNIX

The uximport utility extracts information from the UNIX operating system about the defined users, groups, terminals, hosts, and TCP services. The utility extracts information from NIS, if it is installed, and the system is configured accordingly. It also provides DNS support. You should use uximport as part of the installation procedure.

uximport automatically processed the extracted information to generate selang commands that you can use to add users and groups to the Privileged Access Manager database. The generated commands are printed to the standard output. Use redirection to a file, or pipeline to the selang utility.

This command has the following format:

```
UxImport switches [options]
```

- **-a**  
Generates the selang commands that are required to import users, groups, and hosts, and to join users to their default groups.
- **-c**  
Generates the selang commands that are required to join users to their default groups.

### NOTE

If you also import groups with the -g switch, Privileged Access Manager generates the commands that join users to the groups to which they are explicitly linked.

- **-g**  
Generates the selang commands that are required to import groups from UNIX and NIS to the Privileged Access Manager database.
- **-h**  
Generates the selang commands that are required to import hosts from UNIX, NIS, and DNS to the Privileged Access Manager database. uximport extracts host information from the file /etc/hosts and from NIS, and builds HOST resources. For each host entry in the file /etc/hosts or extracted from NIS, the appropriate newres command is built. Permission to receive any TCP service is assigned to that host.  
In addition, DNS is supported with the -d option. In some machines, information from the file /etc/hosts and NIS is ignored if the specified DNS daemon is running. In Solaris, the information that is gathered depends on the configuration of the system in the file /etc/nsswitch.conf.
- **-t**  
Generates the selang commands that are required to import terminal rules from UNIX and NIS to the Privileged Access Manager database.

uximport extracts host information from the file `/etc/hosts` and from NIS, and builds `TERMINAL` resources. For each entry in the file `/etc/hosts` or extracted from NIS, the appropriate newres `TERMINAL` command is built and permission to log in from the terminal is granted.

In addition, DNS is supported with the `-d` option. In some machines information from the file `/etc/hosts` and NIS is ignored if the specified DNS daemon is running. In Solaris, the information that is gathered depends on the configuration of the system in the file `/etc/nsswitch.conf`.

- **-T**  
Generates the `selang` commands that are required to import TCP services from UNIX and NIS to the Privileged Access Manager database. The names are set according to GECOS in UNIX. The names are truncated to 40 characters if they are longer.
- **-u**  
Generates the `selang` commands that are required to import users from UNIX and NIS to the Privileged Access Manager database. The actual user names are set according to GECOS in UNIX. The names are truncated to 40 characters if they are longer.

#### *options*

- **-d**  
Specifies the use of DNS for generating the list of hosts and terminals to import. Must be accompanied by the `-h` or `-t` switch.
- **-f**  
Skips search for multiple occurrences of the same name. By not using the standard `uximport` processes, this option handles the importing of many users and groups speedily, and saves memory. The `-f` option does not apply to hosts; you should combine them with one or more of the following switches: `-u`, `-g`, or `-a`. Also, use one of these switches when including the `-c` switch with the `-f` option.  
Join and surrogate rules are printed with create records.
- **-G**  
Creates `SURROGATE` class rules for groups. `uximport` adds a record to the `SURROGATE` class for each group it defines, therefore making `SURROGATE` requests protected resources. It also adds rules so that root can surrogate to each of the groups.
- **-gr *n***  
Specifies the number of grace logins for all users, forcing users to change their passwords after *n* logins. This ensures that the `PASSWD_L_C` property in the `USER` record is updated.
- **-o *owner***  
Sets ownership rules for each record. We recommended that you use this option to prevent root from automatically becoming the owner of all the records. *Owner* is the name of the user or group to be assigned ownership of all records that are defined by `uximport`.  
**Note:** You must specify this option as a separate argument followed by *owner*.
- **-pr *groupname***  
Assigns a profile group to users. If you specify this option, Privileged Access Manager uses that group when building the profile of a user. Otherwise, it uses the primary UNIX group.
- **-r**  
Specifies to continue scanning after a failure.
- **-s**  
Creates `SURROGATE` class rules for users and groups. The `uximport` function adds a `SURROGATE` record for every group it defines, thereby making `SURROGATE` requests to the group into protected resources.
- **-U**  
Creates `SURROGATE` class rules for users. `uximport` adds a record to the `SURROGATE` class for each user it defines, therefore making `SURROGATE` requests into protected resources. It also adds rules so that root can surrogate to each of the users.
- **-v**

Displays the status of the program (verbose mode). We recommended that you use this option if your site has many users, groups, or hosts, so that you can verify the progress of the program.

### Example

The following command extracts all information of users, groups, and hosts from the UNIX and NIS databases. It then creates the selang commands that add those records to the database. uximport then creates SURROGATE class records and provides progress indication. Output is directed to the file uxinfo.seos in your home directory.

```
UxImport -a -s -v > ~/uxinfo.seos
```

## uxpatcher Utility

The uxpatcher utility applies a patch to Privileged Access Manager. Use it to apply a patch immediately, or to schedule the application of the patch to occur at the next restart of the product. You can run the utility at any time.

When you schedule uxpatcher to run at the next restart of the product, the seload command checks a staging area for patches. If it detects a patch, it applies the patch before starting the product.

The seload command checks seos.ini for a new token. If the new token is set, then it checks for scheduled patches. The default behavior is not to check for patches, simply to start.

Set the token:

**seini -s seload.allow\_updates 1**

Turn off the token (default):

**seini -s seload.allow\_updates 0**

This command has the following format:

```
uxpatcher -s -x -c <patcher.ini> -r
```

- **-s**  
The patch is deployed to a staging area within the directory structure of the product. For example, if the product path is /opt/CA/PAMSC, then a directory for staging is created in /opt/CA/PAMSC/.pending\_patch. Once the product restarts, seload checks to determine whether it is supposed to check for patches. If so, then seload checks for patches in the staging area and runs all the patches that have the token set to run them. If the patch is applied successfully, the token to run is removed. However, the patch files are not removed. To remove the patch files from the staging area after patching, use the -x flag.
- **-x**  
seload removes the staging area files after it applies the patch.
- **-c**  
Indicates the configuration file. The product is shipped with patcher.ini as the default configuration file, but you can specify a different file.
- **-r**  
Removes the most recently installed patch.

### NOTE

When you use the -s flag, uxpatcher checks the current version of seload to determine if it includes the appropriate functionality. (This is only relevant on 12.8 SP1 and 14.01 because they were shipped without the functionality. SC141 is shipped with that functionality, so not necessary.

When you use the '-s' flag, uxpatcher checks that the patch contains seload. If so, it indicates that this patch must be applied without using the '-s' flag.

### Examples

Run the uxpatcher utility to install a patch immediately:

```
[root@rh74-2-filth02 patcher]# ./uxpatcher -c patcher.ini

CA ControlMinder uxpatcher v12.81.0.3131 - Patch Installer

Copyright (c) 2013 CA. All rights reserved.

Reading patch configuration file 'patcher.ini'

Reading files, section [MandatoryFiles].

    file: /opt/CA/AccessControl/bin/SEOS_syscall.70-3100-693-RHELX86_64.MP.ko version:
    12.81-0  3143

Reading files, section [OptionalFiles].
```

Schedule a new patch for the next restart:

```
[root@rh74-2-filth02 patcher]# ./uxpatcher -s -c patcher.ini

CA ControlMinder uxpatcher v12.81.0.3131 - Patch Installer

Copyright (c) 2013 CA. All rights reserved.

Reading patch configuration file 'patcher.ini'

Reading files, section [MandatoryFiles].

    file: /opt/CA/AccessControl/bin/SEOS_syscall.70-3100-693-RHELX86_64.MP.ko version:
    12.81-0  3143

Reading files, section [OptionalFiles].

Scheduling patch for next restart

Patch          : T47D091
```

Description : Test Patch for new uxpatcher

Product : AC

Build : 12.81-0 (2994)

Backup size : 1 KB

Checking patch data

Patch version matches installed product version.

Patch description matches the platform.

Patch T47D091 will be applied at next product restart.

#### Remove the most recently installed patch:

```
[root@rh74-2-filth02 patcher]# ./uxpatcher -r
```

CA ControlMinder uxpatcher v12.81.0.3131 - Patch Installer

Copyright (c) 2013 CA. All rights reserved.

You are about to remove the last applied patch, i.e. T47D091

Checking if backup files exist in /opt/CA/AccessControl/patch/T47D091

Do you want to remove patch T47D091? [n,y] y

Deleting directory /opt/CA/AccessControl/patch/T47D091

Unregistering patch T47D091

Successfully removed patch T47D091

## Services and Daemons in Detail

This section contains a complete alphabetic reference to all Privileged Access Manager daemons and services.



## Agent Manager Service

### Valid on Windows

The Privileged Access Manager Agent Manager service provides management services for the Privileged Access Manager plug-ins. The Privileged Access Manager Agent Manager service provides the plug-ins with the following services:

- Scheduling service manages the plug-ins schedules.
- Watchdog service verifies that the plug-ins are running and starts up plug-ins after failure.
- Messaging service provides the plug-ins with message queue services and stores messages in case the Enterprise Management Server is unavailable.

The Agent Manager registry key contains registry entries to let you fine-tune the Agent Manager. You can find the key in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager
```

## Message Queues

### Valid on Windows

The Message Queue service manages the Message Queue that handles all inbound and outbound messages between the Enterprise Management Server and other Privileged Access Manager components. The Message Queue has a dedicated queue for each client component that communicates with the Enterprise Management Server, as follows:

- **Report Queue:**  
The Report Queue receives scheduled snapshots of the endpoint databases. The reporting service uses the snapshots to generate enterprise reports.
- **Audit Queue:**  
The Audit Queue receives audit events that occur on the endpoints. You can configure the Audit Log to collect the audit events.
- **Server to Endpoint Queue:**  
The Server to Endpoint Queue receives data from the Deployment Map Server (DMS) and then forwards the data to an endpoint.  
For example: When you deploy a UNAB config policy, the DMS sends the config policy to this queue. The UNAB agent then collects the policy from the queue and deploys the policy on the UNAB endpoint.
- **Endpoint to Server Queue:**  
The Endpoint to Server Queue receives information from endpoints and then forwards the information to the Deployment Map Server (DMS).  
For example, a UNAB endpoint sends a heartbeat notification to this queue. The DMS then collects the heartbeat notification from the queue and updates the endpoint status in its database.

## Web Service

### Valid on Windows

The Web Service manages the web-based applications that you use to manage an enterprise installation of Privileged Access Manager. The web-based applications are installed on the Application Server. The Application Server is installed by default on the Enterprise Management Server.

The Application Server contains the following web-based applications:

- Privileged Access Manager Enterprise Management: Lets you manage policies across your enterprise and configure UNIX Authentication Broker endpoints. Privileged Access Manager Enterprise Management also contains Shared

Account Management (SAM), which lets you manage privileged accounts across the enterprise and acts as a password vault for the privileged accounts.

- Privileged Access Manager Endpoint Management: Lets you administer and configure individual Privileged Access Manager endpoints through a central administration server.
- Privileged Access Manager Password Manager: Lets you manage Privileged Access Manager user passwords. You can modify the password of a Privileged Access Manager user or can force the user to change their own password when they next log in.

The WebService registry key contains registry entries to let you fine-tune the Web Service. You can find the key in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService
```

**Note:** If you install the Enterprise Management Server on a UNIX computer, the eacws daemon manages the web-based applications.

## eacws Daemon

### Valid on UNIX

The eacws daemon manages the web-based applications that you use to manage an enterprise installation of Privileged Access Manager. The web-based applications are installed on the Application Server. The Application Server is installed by default on the Enterprise Management Server.

The Application Server contains the following web-based applications:

- Privileged Access Manager Enterprise Management - Lets you manage policies across your enterprise and configure UNIX Authentication Broker endpoints. Privileged Access Manager Enterprise Management also contains Shared Account Management (SAM). SAM lets you manage privileged accounts across the enterprise and acts as a password vault for the privileged accounts.
- Privileged Access Manager Endpoint Management - Lets you administer and configure individual Privileged Access Manager endpoints through a central administration server.
- Privileged Access Manager Password Manager - Lets you manage Privileged Access Manager user passwords. You can modify the password of a Privileged Access Manager user or force the user to change their own password when they next login.

### NOTE

If you install the Enterprise Management Server on a Windows computer, the Privileged Access Manager Web Service manages the web-based applications.

## KBLAudMgr Daemon Session Logging

### Valid on UNIX

The KBLAudMgr daemon manages the Keyboard Logger session recording agent. You use the Keyboard Logger to track privileged user sessions in UNIX and Linux endpoints. The Keyboard Logger records the interactive session, which you can replay when terminated and send to the Audit Log for analysis.

The [kblaudit] section of the seos.ini file contains tokens that let you fine-tune the Keyboard Logger agent.

## PolicyFetcher Daemon

### Valid on UNIX

The PolicyFetcher daemon performs the following tasks:

- Checks for deviations in the deployed policy at regular intervals
- Looks for deployment tasks on the DH
- Applies policy updates to the local Privileged Access Manager database (seosdb)
- Sends a heartbeat to the DH at regular intervals

Use the start DEVCALC selang command to start the deviation calculator. If you installed advanced policy management on the endpoint, the PolicyFetcher runs the deviation calculator for you.

## ReportAgent Daemon

### Valid on UNIX

The ReportAgent daemon manages the ReportAgent that sends report snapshots and audit events to the Distribution Server for inclusion in Privileged Access Manager, and UNIX Authentication Broker. You run the ReportAgent utility from the *ACSharedDir/bin* directory on a UNIX computer, where *ACSharedDir* is the default directory */opt/CA/PAMSCShared*. You can also use the *report\_agent.sh* script to configure, start, and stop the ReportAgent.

The [ReportAgent] section of the *accommon.ini* file contains tokens that control the behavior of the Report Agent daemon.

## ReportAgent Service (Windows)

### Valid On Windows

The ReportAgent Service manages the ReportAgent that sends report snapshots and audit events to the Distribution Server for inclusion in Privileged Access Manager, and UNIX Authentication Broker. The ReportAgent Service automatically runs on startup if you installed Privileged Access Manager on the endpoint and selected to install the ReportAgent.

The ReportAgent registry key contains registry entries to let you fine-tune the ReportAgent. You can find the key in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent
```

## sepmdd Daemon (UNIX)

The Policy Model daemon.

The sepmdd daemon is the PMDB daemon. The sepmdd daemon performs the following functions:

- Administers the Privileged Access Manager and UNIX databases of the Policy Model.
- Administers the subscriber database.
- Propagates changes from the PMDB to the subscriber databases.

You can find the sepmdd daemon in the *ACInstallDir/bin* directory. The daemon starts the PMDB if it is already created.

- **Syntax**

```
sepmdd policyModel
```

- **Parameters**

- *policyModel*  
The name of the Policy Model.

- **Other Files**

No other special files are used.

**NOTE****NOTE**

When you use `selang` and choose a Policy Model as your target (using hosts `pmd@hostname`), queries to `sepmdd` apply to the PMDB.

Queries do not apply to the various subscriber databases.

- Ensure that a PMDB does not become a subscriber of itself. If a PMDB is subscribed to itself, the Policy Model may block or the network may become overloaded, filling the disk in the process.
- When updating a Policy Model in the UNIX environment of `selang`, do not specify more than one user in the `newusr` command, or specify more than one group in the `newgrp` command.
- When updating UNIX file attributes from `selang`, the Policy Model generates a message stating that the command was passed to its subscribers.
- When working on a Policy Model, you cannot query the status of UNIX file attributes.
- If you set the value of `_shutoff_timeout_` to zero, the `sepmdd` daemon remains up and running indefinitely until you shut it off manually. Use the command `sepmdd -k` to shut down the Policy Model daemon.

**How sepmdd Works**

The Privileged Access Manager agent, `seagent`, starts `sepmdd`; You do not need to run `sepmdd` explicitly. The `sepmdd` daemon runs under the logical user id `_seagent` for Privileged Access Manager, and with the user id `root` in UNIX. You cannot designate another logical user under which `sepmdd` runs.

The PMDBs are stored in a common directory. Specify the name of the common directory with the `_pmd_directory_` token in the `[pmd]` section of the `seos.ini` file, on the station where the Policy Models reside. Each Policy Model resides in a subdirectory of the common directory. The name of the Policy Model is the name of the subdirectory in which it resides.

When `sepmdd` starts, it checks whether any subscriber databases need updating, and updates them if necessary. After this startup process, `sepmdd` waits for user requests. These requests are sent by the Policy Model management program, `sepmdd`, and by the `selang` utility, using `seagent`.

When `sepmdd` receives a request, it applies the request to the PMDB and it sends the result back to the user. If the request should be propagated, `sepmdd` propagates the update to its subscriber databases.

The `sepmdd` daemon attempts to update a subscriber database for the period that is specified in the `_QD_timeout_` token. If the maximum time elapses and the daemon does not succeed in updating a subscriber, it skips that particular subscriber and tries to update the remainder of the subscribers on its list. After it completes its first scan of the subscriber list, `sepmdd` then performs a second scan. During the second scan, it tries to update the subscribers that it did not succeed in updating during its first scan. During the second scan, it tries to update a subscriber until the connect system call times out (approximately 90 seconds).

**NOTE**

The `_QD_timeout_` token may exist in both the `seos.ini` and `pmd.ini` files. If it does, `sepmdd` uses the value in the `pmd.ini` file.

If a subscriber is unavailable during the second scan, `sepmdd` attempts to send it updates every 30 minutes. To modify this interval, set the `_retry_timeout_` token. Because the updates must be sent in the order in which they are received, `sepmdd` does not send subsequent updates to the subscriber database until it becomes available.

If you set the `pull_option` token in the `[pmd]` section of the subscriber database's `seos.ini` file to `yes`, the subscriber database is updated as soon as possible. `seagent` informs the parent Policy Models that the host is up for every Policy Model on the machine, and that its subscriber PMDBs are up, and `sepmdd` sends the update immediately.

Whenever `sepmdd` fails to update a subscriber database, it writes a warning message in the Policy Model error log. For more information about the Policy Model error log see the *Endpoint Administration Guide for UNIX*.

Privileged Access Manager attempts to qualify subscribers as they are added or deleted from the Policy Model.

To remove a subscriber from the list of unavailable subscribers, enter the following command:

```
sepmc -r policyModel subscriber
```

If a subscriber database rejects an update, as can occur if the subscriber database differs from the PMDB, sepmc writes an error message in the Policy Model error log and continues.

To view the error log, enter the following command on the host where the PMDB resides, enter:

```
sepmc -e policyModel
```

You can have sepmc automatically shut itself down after a period of inactivity. By default, however, sepmc does not shut itself down. If you want sepmc to shut itself down, set the `_shutoff_time_` token to a value greater than 0. This value indicates the minutes of inactivity that is allowed before sepmc shuts itself down. To shut sepmc down manually, enter:

```
sepmc -k policyModel
```

### **WARNING**

Do *not* use the UNIX command `kill -9` to shut down sepmc manually; this may destroy the PMDB.

## **UID/GID Synchronization**

As an administrator, you receive messages that refer to users by UID and to groups by GID. Verify that the UIDs and GIDs have the same meaning everywhere.

By default, the PMDB attempts to use the same UIDs and GIDs for new users and groups everywhere. You can help by providing the necessary conditions from the start as follows:

- Start with identical passwd files and identical group files.
- Make sure that the `synch_uid` token in the `pmd.ini` file is set to yes.

You can depend on compatibility between the UIDs and between the GIDs of your local database, your PMDB, and your PMDB subscribers if the following conditions exist:

- Your local database is a subscriber to your PMDB
- The PMDB is the only source of new users and new groups for your subscriber databases

If you create a user with a UID that is already in use in the PMDB or in some other subscriber computer, the individual update of the subscriber fails. In all other subscriber computers where no such conflict exists, the update succeeds.

An alternative to synchronizing your passwd and group files is to specify the UID of each new user and the GID of each new group explicitly.

## **Filter Mechanism**

You may want your PMDB to update the subscriber stations below it selectively. To define which records are sent to the subscriber stations, point the filter token in the `pmd.ini` file to a filter file. Updates to the subscriber stations are then limited to the records that pass the filter file.

A filter file consists of lines with six fields per line. The fields contain the following information:

- The form of access that is permitted or prohibited. The possible values are AUTHORIZE\_DELETE, AUTHORIZE\_MODIFY, CREATE, DELETE, DEPLOY, EDIT, FILESCAN, GET, SEOS\_ACCS\_READ, JOIN\_DELETE, JOIN\_MODIFY, MODIFY, READ, START, or UNDEPLOY.
- The environment that is affected. The possible values are AC, CONFIG, UNIX, NT, or NATIVE
- The class of the record. The possible values include all classes in Privileged Access Manager, including user-defined classes.
- The objects within the class that the rule covers. For example, User1, AuditGroup, or TTY1
- The properties that the record grants or cancels. For example, OWNER and FULL\_NAME in the filter line for user records means that any command having those user properties are filtered. You must enter each property exactly.
- Whether such records should be forwarded to the subscriber station or not. The possible values are PASS or NOPASS

You can use an asterisk in any field to mean all possible values. If more than one line covers the same records, the first applicable line is used.

In each line of the filter file, spaces separate the fields. In fields with more than one value, semicolons separate the values. Any line beginning with # is considered a comment line. Empty lines are not allowed. Here is an example of a line from a filter file:

CREATE	AC	USER	*	FULL-NAME;OBJ_T YPE	NOPASS
<i>form of access</i>	<i>environment</i>	<i>class</i>	<i>record name ( * =all)</i>	<i>properties</i>	<i>treatment</i>

For example, suppose that the file with this line is named TTY1\_FILTER, and the pmd.ini file of the Policy Model TTY1 contains the line filter=/opt/CA/PAMSC/TTY1\_FILTER. The Policy Model TTY1 does not send records that create Privileged Access Manager users with the FULL\_NAME and OBJ\_TYPE (Admin, auditor, and so on). The asterisk means regardless of name.

The following list shows the selang commands that are relevant for each access value:

Access	selang Command
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres, newusr, newgrp, newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
DEPLOY	deploy
EDIT	editres, editusr, editgrp, editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres, chusr, chgrp, chfile, join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (undeploy)

Privileged Access Manager does not validate rules. If you enter an invalid value in a rule, the rule never matches an update transaction.

## Policy Model Service (sepmdd)

### Valid on Windows

Privileged Access Manager Policy Model Service (sepmdd) is the PMDB service. This service performs the following functions:

- Administers the Privileged Access Manager and Windows databases of the Policy Model
- Administers the subscribers database
- Propagates changes from the PMDB to the subscriber databases

SeOSAgent starts the sepmdd service. There is no need to run sepmdd explicitly. The two possible states for each Policy Model are Started and Stopped.

The PMDBs are stored in a common directory. The registry value `_pmd_directory_` in the subkey `HKLM\Software\ComputerAssociates\AccessControl\Pmd` specifies the name of the common directory. Each Policy Model resides in a subdirectory of the common directory. The name of the Policy Model is the name of the subdirectory in which it resides.

When sepmdd starts, it checks whether any subscriber databases need to be updated. If necessary, it updates them. After this startup process, the sepmdd service waits for user requests. User requests are sent by the Policy Model management utility `sepmdd` and by `selang` using the Privileged Access Manager Agent.

When a request is received, sepmdd applies it to the PMDB and sends the result back to the user. If the request should be propagated, sepmdd propagates the update to its subscriber databases.

The sepmdd service tries to update a subscriber database for 30 seconds. If this elapses and the service does not succeed in updating a subscriber, it skips that particular subscriber and tries to update the remainder of the subscribers on its list. After it completes its first scan of the subscriber list, sepmdd then performs a second scan, in which it tries to update the subscribers that it did not succeed in updating during its first scan. During the second scan, it tries to update a subscriber until the connect system call times out (approximately 90 seconds).

If a subscriber is unavailable during the second scan, sepmdd attempts to send it updates every 30 minutes.

Because the updates must be sent in the order in which they are received, sepmdd does not send subsequent updates to the subscriber database until it becomes available.

Each time sepmdd fails to update a subscriber database, a warning message is written in the Policy Model error log.

### Filter Mechanism

You may want your PMDB to update the subscriber stations below it selectively. To define which records to be sent to the subscriber stations, set the registry key string value to a filter file. Updates to the subscriber stations are then limited to the records that pass the filter file.

Here is an example:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd\PolicyModelName\Filter
```

A filter file consists of lines with six fields per line. The fields contain this information:

- **The form of access permitted or prohibited**  
Valid values are: `AUTHORIZE_DELETE`, `AUTHORIZE_MODIFY`, `CREATE`, `DELETE`, `DEPLOY`, `EDIT`, `FILESCAN`, `GET`, `SEOS_ACCS_READ`, `JOIN_DELETE`, `JOIN_MODIFY`, `MODIFY`, `READ`, `START`, or `UNDEPLOY`.
- **The environment affected**  
Valid values are: `AC`, `CONFIG`, `UNIX`, `NT`, or `NATIVE`.
- **The class of the record**  
Valid values include all classes in Privileged Access Manager, including user-defined classes.
- **The objects within the class that the rule covers**

For example: User1, AuditGroup, or COM2.

- **The properties that the record grants or cancels**

For example, including GROUPS and FULLNAME in the filter line for user records means that any command having those user properties is filtered. You must enter each property exactly as it appears.

- **Whether such records should be forwarded to the subscriber station**

Valid values are: PASS, NOPASS

**NOTE**

You can use an asterisk to mean all possible values in any field. If more than one line covers the same records, the first applicable line is used.

**NOTE**

In each line of the filter file, spaces separate the fields. In fields with more than one value, separate the values with semicolons. Any line beginning with # is considered a comment line. Empty lines are not allowed. Here is an example of a line from a filter file:

CREATE	AC	USER	*	FULLNAME;OBJ_T YPE	NOPASS
form of access	environment	class	record name ( * =all)	properties	treatment

If, for example, the file with this line is named Printer1\_Filter.flt and the registry key HKEY\_LOCAL\_MACHINE\Software\ComputerAssociates\AccessControl\Pmd\PM-\Filter contains the line C:\Program Files\CA\PAMSC\data\Printer1\_Filter.flt, then Policy Model PM-1 does not send records that create Privileged Access Manager users with the FULLNAME and OBJ\_TYPE (admin, auditor, and so on). The asterisk means regardless of name.

The selang commands that are relevant for each access value are:

Access	selang Command
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres, newusr, newgrp, newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
DEPLOY	deploy
EDIT	editres, editusr, editgrp, editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres, chusr, chgrp, chfile, join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (undeploy)

**NOTE**

Privileged Access Manager does not validate rules; therefore, if you enter an invalid value in a rule, the rule will never match an update transaction.

## Registry Subkeys

Each PMDB has its own registry subkey under:



```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd
```

This subkey contains the values that define and determine the activity of the PMDB. The `sepmdd` utility creates a subkey, if it does not already exist, with the minimum number of entries needed.

- **Notes**

- When you use `selang` and choose a Policy Model as your target (using hosts `pmd@hostname`), queries to `sepmdd` apply to the PMDB but not to the various subscribers' databases.
- Ensure that a PMDB does not become a subscriber of itself. If a PMDB is subscribed to itself, the Policy Model may block or the network may become overloaded, filling the disk in the process.
- You cannot specify more than one user with the `newusr` command when you are working in the UNIX environment using `selang` to update a Policy Model.
- You cannot specify more than one group in the `newgrp` command when you are working in the UNIX environment using `selang` to update a Policy Model.
- When updating UNIX file attributes from `selang`, the Policy Model generates a message stating that the command has been passed to its subscribers.
- When working on a Policy Model, you cannot query the status of Windows file attributes.
- The `sepmdd` service remains active indefinitely until deactivated with the `-k` options.

## seagent Daemon

### Valid on UNIX

The `seagent` daemon accepts requests from remote stations, and applies them to the local Privileged Access Manager and UNIX databases, or to the PMDBs. This daemon also checks that the Watchdog daemon `seoswd` is running, and if it is not, restarts it.

#### NOTE

When you load Privileged Access Manager (`seload`) it also starts `seagent`; this daemon does not work independently and cannot be started using the `seagent` command.

`Seagent` waits for connections on the `seoslang2` TCP service (whose default value is 8891). When a connection request arrives, `seagent` forks a child process to handle the communication on the connection, and continues waiting for new connections.

The child processes of `seagent` get the requests from the client, and apply them to the local database.

The Agent is also responsible for the following points:

- Updating the UNIX user file `/etc/passwd`, the system shadow password file, and the UNIX group file `/etc/group`
- Alerting Policy Model daemons when an update is sent
- Alerting the parent Policy Models of both the local host and any Policy Model on the machine when a subscriber station (that has been down) is available for updating

Privileged Access Manager uses only port 8891. We recommended that you do not change this port.

The `seagent` agent uses the RPC mechanism and therefore the portmapper must be running on the local machine. For more information about the portmapper, check your system documentation.

This command has the following format:

```
seagent
```

**NOTE**

- [seoswd Daemon](#)
- [sepmdd Daemon \(UNIX\)](#)

**CA Privileged Access Manager Server Control Agent****Valid on Windows**

The Privileged Access Manager Agent service communicates with Privileged Access Manager clients through a proprietary application protocol over TCP/IP and manages security for Windows native resources. The Privileged Access Manager Agent service also checks that the Watchdog service is running, and if it is not, restarts it.

**NOTE**

When you load Privileged Access Manager it also starts the agent service; this service does not work independently.

You can run Privileged Access Manager agent service from a command-prompt window. This command has the following format:

```
seagent [start|remove|debug]
```

- **Start**  
Specifies to start the Privileged Access Manager agent service
- **Remove**  
Specifies to remove the Privileged Access Manager agent service from the operating system
- **Debug**  
Specifies to run the Privileged Access Manager agent service as a console for debugging purposes

**seosd Daemon****Valid on UNIX**

The Privileged Access Manager authorization daemon. The executable file seosd is the main Privileged Access Manager daemon. A daemon is a process that has disconnected from both its controlling TTY and its parent process. The Privileged Access Manager daemon makes the runtime decisions that are required to grant or deny access to a resource.

Only root can invoke seosd, and only a user with the ADMIN or OPERATOR attribute can shut it down.

The Privileged Access Manager daemon opens, reads, and updates the database. No other process can access this database while the Privileged Access Manager daemon is running. The Privileged Access Manager daemon also blocks any write, delete, or rename access to critical files. These files include the Privileged Access Manager audit and trace files and, optionally, the Privileged Access Manager binary files.

The seosd executable becomes a daemon only if one or both of the following conditions are true:

- The trace messages are not sent to the screen. You set the trace\_to token in the seos.ini file to *file*, *file*, *stop*, or *none*.
- You specify no argument (except-d) on the command line when invoking the utility.

If none of these conditions are true, seosd remains a regular process, which is connected to the terminal from which you invoked it.

During startup, seosd also invokes the following processes:

- seagent, the Privileged Access Manager agent daemon.
- seoswd, the Privileged Access Manager watchdog daemon.

The Privileged Access Manager daemon is initialized only after these daemons are also running. After initialization, these three daemons maintain a type of handshaking protocol to ensure that they are all alive and responding. If one of these daemons is found to be absent, one of the other two daemons automatically restarts it.

This command has the following format:

```
seosd [-d|argument]
```

#### NOTE

If you enter seosd with no arguments, it runs seosd as a daemon.

- *argument*  
Ignored. However, if you specify an argument, seosd remains a regular process.
- **-d**  
Runs seosd as a daemon and forces tracing to the trace\_file.

## Authorization Engine Service

### Valid on Windows

The Privileged Access Manager authorization engine manages access request decisions and database updates.

The Privileged Access Manager engine opens, reads, and updates the database. No other process can access this database while the Privileged Access Manager engine is running. The Privileged Access Manager engine also blocks any write, delete, or rename access to critical files. These files include the Privileged Access Manager audit and trace files and, optionally, the Privileged Access Manager binary files.

During startup, the engine service also invokes the following services:

- The Privileged Access Manager agent service.
- The Privileged Access Manager watchdog service.

The Privileged Access Manager engine service is initialized only after these services are also running. After initialization, these three services maintain a type of handshaking protocol to ensure that they are all alive and responding. If one of these services is found to be absent, one of the other two services automatically restarts it.

This command has the following format:

```
Seosd -start [<counter>]
Seosd -debug
```

- **-start [<counter>]**  
Starts Privileged Access Manager services and waits for a specified interval to verify that the services started.

#### NOTE

If you do not specify <counter>, Privileged Access Manager does not wait to check whether the services started.

- **-debug**  
Runs the utility as a console application for debug purposes.

#### NOTE

If you run seosd without any arguments, seosd executes as a service.

## selogrcd Daemon Collect Audit Records

### Valid on UNIX

Collector daemon for the Privileged Access Manager log routing system.

**Note:** selogrcd does not work in IPv6-only environments.

The Privileged Access Manager log routing daemons, selogrd and selogrcd, provide system administrators with convenient, selective access to the audit log records.

The selogrcd utility is the collection daemon. This daemon collects the selected audit log records sent by various satellite systems and stores them in the audit collection file. The default file is *ACInstallDir/log/seos.collect.audit*.

Two tokens enhance audit collection file management. Both tokens are in the [selogrd] section of the seos.ini file

- Use the Caudit\_size token to specify the maximum size of the audit collection file. When the file reaches this size, Privileged Access Manager creates a backup file and opens a new file.
- Use the CbackUp\_Date token to specify an automatic backup interval and timestamp for the audit collection file.

You can force selogrcd to start a new audit file by sending it a USR1 signal. Once you have the selogrcd process ID, send it a USR1 signal using a kill command such as:

```
kill -USR1 processID
```

When it receives a USR1 signal, selogrcd renames the existing audit file to *ACInstallDir/log/seos.collect.bak* and creates an audit file. You can also use a cron job to perform this task periodically. A sample script that performs this task is provided in the directory *ACInstallDir/samples/selogrcd*.

### NOTE

You can expand the functionality of the selogrcd daemon by writing programs at your site that use the APIs provided with Privileged Access Manager. For more information, see the *SDK Guide*.

This command has the following format:

```
selogrcd [-d] [-l lock-file-name]
```

- **-d**  
Specifies the debug mode. In this mode, selogrcd does not become a daemon. It sends debug information to the terminal.
- **-h**  
Displays the help for this utility.
- **-l lock-file-name**  
Specifies the name of the lock file to be used (*lock-file-name*). By default, selogrcd uses the file *ACInstallDir/lock/selogrcd*.

### NOTE

If you set selogrd to work on a different log file (such as a PMDB log file), the lock file has an extension based on the PMDB name or the data file name that was used as the parameter for the [selogrd command](#).

## selogrd Daemon Emit Audit Records

### Valid on UNIX

Emitter daemon for the Privileged Access Manager log routing system.

**Note:** selogrd does not work in IPv6-only environments.

The Privileged Access Manager log routing, daemons selogrd and selogrcd, provide system administrators with convenient, selective access to the audit log records.

The selogrd utility is the emitter daemon. This daemon performs the following tasks:

- Distributes selected local audit log records to the various destination hosts
- Reformats audit log records into email messages, ASCII files, or user windows
- Sends out notification messages that are based on audited events

#### NOTE

The Privileged Access Manager daemon must be up and running before the log routing daemons can collect any meaningful information on Privileged Access Manager events. If the Privileged Access Manager daemon is not running, selogrd routes only old audit records.

The log routing daemons use a configuration file to determine where each audit log record is sent, the format in which the log record is written, and which records are routed. By default, selogrd uses the *ACInstallDir/log/selogrd.cfg* audit log route configuration file. The names of the configuration file and other global environment variables that selogrd and selogrcd use are specified in the Privileged Access Manager initialization file, *seos.ini*.

The selogrd daemon periodically restarts and reads the configuration file. In addition, you can force the selogrd daemon to restart at a specified time. To do so, you must send the following HUP signal:

```
kill -HUP processID
```

- *processID*  
Defines the selogrd process ID. (Use the UNIX *ps* command to find it; see your UNIX documentation for more information.)

The selogrd utility provides API access for programmers working under Privileged Access Manager. The Logroute API allows programmers to incorporate their own options into the Privileged Access Manager audit log system to support in-house alerts that are not provided by the current log-routing facility. The Logroute API also allows programmers to use the log routing daemons to provide functions to their own programs. For more information about all the Privileged Access Manager APIs, see the *SDK Developer Guide*.

This command has the following format:

```
selogrd [-audit fileName] [-config fileName] [-d] \
[-data fileName] [-pmdb policy-model-name]
```

- **-audit *fileName***  
Defines the audit file to use instead of the file that is listed in *seos.ini* for the input audit file.
- **-config *fileName***  
Defines the configuration file to use instead of the file that is listed in *seos.ini* for the configuration file.
- **-d**  
Specifies to print debug messages.
- **-data *fileName***  
Defines the data file to use instead of the file that is listed in *seos.ini* to store routing progress information.
- **-h**  
Displays the help for this utility.
- **-pmdb *policy-model-name***  
Instructs selogrd where to route audit data from a PMDB. The command tells selogrd to send audit data from the PMDB that you specified in the command, to the audit file that you specified in the *audit\_log* token in the *pmd.ini* file of the PMDB.  
By default, selogrd uses the data file and lock file that consist of the Policy Model name. If you specify the data file or lock file or both on the command line, those files override the default values. The lock file and data file names should be different from those of the selogrd that route the audit data of the station. selogrd can only support Policy Model names of 12 characters.  
The audit data that is sent from a PMDB appears in the collected audit file as if it comes from a station with the name *policy-model-name@station-name*

## Task Delegation Service

### Valid on Windows

The task delegation service (SeSudo.exe) grants the required rights and privileges to ordinary users to enable them to perform administrative tasks while not being members of Windows high privileged groups. Example: the Administrators group.

When a user attempts to perform an administrative task, such as to start or stop a Windows service, the task delegation service performs these tasks:

1. Communicates with the Privileged Access Manager engine service to verify that the user has is authorized to perform the task.
2. The Privileged Access Manager engine service does the following:
  - a. If the user is authorized to run the task, the Privileged Access Manager engine service authorizes the task delegation service to run the task.
  - b. If the user is not authorized to run the task, the Privileged Access Manager engine blocks the attempt.

Run the Privileged Access Manager task delegation service from a command-prompt window using the `sesudo` command. This command has the following format:

```
sesudo [-do [record] [parameters]] -list | -h]
```

- **-do [record] [parameter]**  
Specifies to execute the commands that are embedded in the [record] field with additional parameters
- **-list**  
Specifies to display a list available records that the user can execute
- **-h**  
Specifies to display the command help menu

### seoswd Daemon

#### Valid on UNIX

The Privileged Access Manager watchdog daemon.

The watchdog (seoswd) monitors the file information and digital signatures of programs that are defined in the database as trusted programs. Monitoring is performed in the background with a minimal load on the system. The Privileged Access Manager agent daemon seagent automatically starts seoswd.

The seoswd daemon performs the following functions:

- Monitors the programs that you defined in the PROGRAM class of the database. If the watchdog detects that a program was modified, it notifies the Privileged Access Manager daemon, seosd, which marks the program as

untrusted. The seosd daemon does not allow an untrusted program to run. The seosd daemon also marks the program's status change to untrusted in the database and creates an audit record.

- Monitors files that are defined as secured files. These files are defined in the SECFILE class in the database.
- Monitors seosd to ensure it is running. If the watchdog detects a problem with seosd, it automatically restarts it.
- The seoswd daemon uses the system log syslogd to notify the security administrators when it detects that seosd has stopped responding. All system log messages are submitted as AUTH facility. For more information on the system log facility, see your system man pages under the syslogd and syslog.conf sections.
- Reports several events to Privileged Access Manager, and creates audit records for programs and secured files that were found to be altered.
- Allows you to specify interval and fixed scanning schedules for trusted programs and secure files.
- The watchdog ignores any signal except SIGHUP; you cannot kill the seoswd daemon unless you first shut down seosd. However, if you execute the command `kill -SIGHUP pid`, the watchdog scans all trusted programs and secure files in the database.

There are two ways in which you can set up the Watchdog scanning mechanism:

1. Determine a start time and then repeat scans at a given interval.  
For example, when checking trusted programs, the Watchdog will start the first scan at *PgmTestStartTime* and will check all the trusted programs. Rescanning will take place *PgmTestInterval* seconds after the beginning of the previous scan.
2. Scan at given times.

#### NOTE

In both cases, the Watchdog will sleep periodically for a predetermined rest period (*PgmRest* seconds) during each scan. The Watchdog rests in order to prevent system overload.

You can choose to use one mechanism or both simultaneously. For example, starting at 12:00, scan every 4 hours as well as at 13:00 and 17:30.

In addition to the above mentioned mechanisms for routine scanning of the trusted programs and secured files, there is a way to perform a one-time scan on demand by sending a HUP signal (see token *SignalMinInterval*).

If you invoke seoswd without an argument, it runs as a daemon. If you invoke seoswd with the `-d` argument, it runs as a daemon, but displays all debug information on the terminal from which you invoked it.

## Watchdog Service

### Valid on Windows

The watchdog monitors the file information and digital signatures of programs that are defined in the database as trusted programs. Monitoring is performed in the background with a minimal load on the system. The Privileged Access Manager agent service automatically starts the watchdog service.

The watchdog service performs the following functions:

- It monitors the programs that you defined in the PROGRAM class of the database. If the watchdog detects that a program was modified, it notifies the Privileged Access Manager Engine, which marks the program as untrusted. The

engine service does not allow an untrusted program to run. The engine service also marks the status change of the program to untrusted in the database and creates an audit record.

- It monitors files that are defined as secured files. These files are defined in the SECFILE class in the database.
- It monitors the Privileged Access Manager engine service to ensure it is running. If the watchdog detects a problem with the service, it automatically restarts it.
- The service uses the system log to notify the security administrators when it detects that the engine service has stopped responding. All system log messages are submitted as AUTH facility.
- It reports several events to Privileged Access Manager, and creates audit records for programs and secured files that were found to be altered.
- It allows you to specify interval and fixed scanning schedules for trusted programs and secure files.

You can run Privileged Access Manager watchdog service from a command-prompt window. This command has the following format:

```
seoswd [start|remove|debug]
```

- **Start**  
Specifies to start the Privileged Access Manager watchdog service
- **Remove**  
Specifies to remove the Privileged Access Manager watchdog service from the operating system
- **Debug**  
Specifies to run the Privileged Access Manager watchdog service as a console for debugging purposes

## uxchecklogin Utility

### Valid on UNIX

The UNAB uxchecklogin utility simulates a user login to the endpoint. It is a useful tool for troubleshooting login problems. This utility drives the Pluggable Authentication Modules (PAM) stack using arguments that you specify on the command line and displays results of the integration progress from a particular service.

This command has the following format:

```
uxchecklogin [-u <user> [-w <password>]] [-s <servicename>] [-l <loops>] [-nonstop]
```

- **-u <user>**  
A username. If you do not supply a username, a temporary local user is created local storage. The username is used for the test, and deleted when the test is complete.
- **-w <password>**  
A user password. If you do not supply a password here, you supply one during the test.
- **-s <service>**  
The name of a service that is used for the test.
- **-l <loops>**  
The number of calls to the entire Pluggable Authentication Modules stack. By default, the Pluggable Authentication Modules stack is called once.
- **-nonstop**  
Do not stop the test because of Pluggable Authentication Modules stack returned values.

### Example

This example uses the username georgew and the sshd service.

```
/tmp> uxchecklogin -s sshd -u georgew
```



CA ControlMinder UNAB uxchecklogin v14.1.00.000 - Check user login

Copyright (c) 2013 CA. All rights reserved.

Password for georgew:

pam\_start OK.

pam\_set\_item PAM\_RHOST OK

pam\_set\_item PAM\_RUSER OK.

pam\_set\_item PAM\_TTY OK.

pam\_set\_item PAM\_OLDAUTHTOK OK.

pam\_set\_item PAM\_AUTHTOK OK.

-- Calling PAM stack --

Calling pam\_authenticate()

my\_converse() called, style of first msg is 1.

asked to prompt: 'Password: '

returning: '\*\*\*\*\*'

pam\_authenticate() returned PAM\_SUCCESS

Calling pam\_acct\_mgmt()

pam\_acct\_mgmt() returned PAM\_SUCCESS

Calling pam\_setcred()

pam\_setcred() returned PAM\_SUCCESS

```
Calling pam_open_session()

pam_open_session() returned PAM_SUCCESS

-- End of PAM stack call --

Test ended, return code is PAM_SUCCESS.
```

## postupdate-nss-gr Utility

### Valid on UNIX

The postupdate-nss-gr utility remaps UNAB-managed group data. Remapping uses the group name as the key while searching for an entry to be changed. It can modify name and gid attributes or both. To enable remapping, fill out the nss\_cache\_update\_post\_job token in the uxauth.ini file with the name of the postupdate-nss-gr utility. See [The uxauth.ini File](#).

The utility can be run in two modes: data preparation (data dump) and data remapping.

This utility has the following syntax:

```
postupdate-nss-gr -dump -v
```

- **-dump**Creates a template input file.
- **-v**Displays the mapped data and any mapping errors. You can remap group data in nss.db from the command line, with postupdate-nss-gr, rather than through the agent during UNAB runtime.

### Example

1. The following command creates the AD group data template for editing in /opt/CA/uxauth/etc/update-nss-gr.input:

```
/tmp> postupdate-nss-gr -dump
```

2. Initial data for groups that are being remapped (shown for Solaris):

```
/tmp> getent group | egrep 'staff|ingres|dba'

staff::1:

ingres::201:

dba::206:
```

```
dbadmin::61098:
```

```
busdba::61127:
```

3. The following is the content of the input file /tmp> head -12 /opt/CA/uxauth/etc/update-nss-gr.input:

```
#####
#          CA Technologies, Inc.   (c) 2017          #
#  #
#  Remapping rules for names and gid settings of AD groups in      #
#  UNAB's nss.db database.  Lines that start with # are comments.  #
#  A new setting of - means that the current value should remain   #
#  as is.  Group names are indexed, so they should be unique.     #
#####
#  Current name      =>  new group name          curgid => newgid
staff                =>  -                        ##   100 => -
ingres               =>  -                        100 => -
dba                  =>  -                        206 => -
```

4. The following is an example of the input file after editing:

```
#####
#          CA Technologies, Inc.   (c) 2017          #
#  #
#  Remapping rules for names and gid settings of AD groups in      #
#  UNAB's nss.db database.  Lines that start with # are comments.  #
#  A new setting of - means that the current value should remain   #
#  as is.  Group names are indexed, so they should be unique.     #
#####
```

#	Current name	=> new group name	curgid => newgid
	staff	=> ad_staff	100 => -
	ingres	=> ad_ingres	100 => 100
	dba	=> -	206 => 100

**NOTE**

Group names must comply with operating system restrictions, such as group name length. When entering new group names or a group id, consider that the UNIX/Linux name switch (NSS) facility exhibits an "aliasing" effect when several groups have the same group id.

5. You can apply mappings immediately, or by the agent during UNAB runtime. Applying them immediately can verify that mapping rules work as expected. The agent applies the mapping rules directly rather than through the corresponding update tool. The agent applies mapping rules to nss.db as a post update after it gets the data from AD. In the example below, the utility uses the -v argument to show its actions and warn about malformed input lines:

```
/tmp> postupdate-nss-gr -v

Changed group 'staff' attributes to ('ad_stuff', 100)

Changed group 'ingres' attributes to ('ad_ingres', 100)

Changed group 'dba' attributes to ('dba', 100)
```

**Using the Sekmodutil Tool**

The sekmodutil tool lists SEOS kernel modules for the current system, or for a specific OS, distribution or release. In addition, it allows users to remove unrelated kernel modules to save disk space. This tool can be distributed as a standalone tool to the existing installations and it will be included in the full installation package. You can access the following information by using the "sekmodutil -h".

**NOTE**

This tool has been integrated into the installers, both legacy installation and native installation, for Linux to remove kernel modules that support Linux distros other than the current system. By default, installers will remove unrelated modules. When doing installation interactively, the installer will prompt the following messages and the user can choose to keep those modules or not.

```
-----[ Clean up SEOS_syscall Modules ]-----
For Linux, the installer will install all SEOS_syscall modules from the
installation package.
This includes modules for other Linux distributions. For example, modules for
SLES, Oracle
Linux, or Ubuntu will also be installed on an RHEL system.

Do you want to keep unrelated SEOS_syscall modules? [N/y]:
```

During the installation, sekmodutil installs under the lbin subdirectory. The installer also creates sekmodcleanup as a symbolic link to sekmodutil. When running sekmodcleanup, it runs as "sekmodutil -x" to remove unrelated modules of the current system.

## Usage

This script, by default, lists SEOS\_syscall kernel modules for the specific OS and distro, if applicable, in the installed or specified directory.

```
Usage: sekmodutil [-D install_bin_dir] [-o OS] [-d distro]
        [-r major_release] [-m] [-x]
```

```
sekmodutil [-h]
```

## Arguments

- h      Print usage. All other arguments will be ignored.
- D install\_bin\_dir  
      Specify the directory where SEOS\_syscall modules are installed. If not specified, the default is the current installation bin directory.
- o OS  
      Select SEOS\_syscall modules for the specified OS. If not specified, the default is the current system. Valid values are: Linux, SunOS (Solaris), AIX or HP-UX. (case insensitive)
- d distro  
      For Linux only. Specify the distribution of the Linux system. This will be ignored if the OS is not Linux. If not specified and the current system is not Linux, this script will terminate with an error. If not specified and the current system is Linux, the default is the current system's distribution. Valid values are: Redhat, RHEL, Suse, SLES, Oracle, OEL, Ubuntu, CentOS, VMware or Debian. (case insensitive)
- r major\_release  
      Specify the major release. If not specified and the current system's OS matches with the OS specified, the default is the current system's release. If not specified and the current system's OS does not match with the OS specified, the default is all. Valid values are:  
       Redhat/Oracle/CentOS: 5, 6, 7, 8 or all  
       SuSE: 10, 11, 12, 15 or all  
       Ubuntu: 12.04, 14.04, 16.04, 17.04, 18.04 or all  
       Solaris: 8, 9, 10, 11 or all  
       AIX: 5.2, 5.3, 6.1, 7.1, 7.2 or all  
       HP-UX: 11.11, 11.23, 11.31 or all

This argument does not support VMware or Debian.

-x  
Remove all other modules. This argument will be ignored if the kernel module for the current host system could be removed.

### Examples

1. To list related SEOS kernel modules for the current host system: # sekmodutil
2. To list related SEOS kernel modules for the current host system and remove unrelated modules: # sekmodutil -x
3. To list SEOS kernel modules for RHEL 7: # sekmodutil -o linux -d rhel -r 7
4. To list SEOS kernel modules for all versions of Oracle Linux, # sekmodutil -o linux -d oracle -r all
5. To remove kernel modules that support other Linux distro, # sekmodutil -r all -x

## Audit Log Records

### Audit Event Types

The information Privileged Access Manager stores in the audit log is determined by the type of event it audits.

### Login Event

Login events describe an attempt to log in to Privileged Access Manager or a Privileged Access Manager protected host.

Audit records in this event have the following format:

```
Date Time Status Event UserName SessionID Details Reason Terminal Program AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Values:** Can be one of:

- D (Denied) Denied the event because of insufficient authorization.
- P (Permitted) Permitted the event.
- W (Warning) Permitted the event because Warning mode is set although the access request violates an access rule.

- **Event**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **UserName**

Identifies the name of the accessor that performed the action that triggered this event.

- **SessionID**

Identifies the accessor's session ID.

**NOTE**

By default this field does not appear in a non-detailed seaudit output. To display this field in a non-detailed seaudit output, specify the `-sessionid` option in the seaudit command.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run `seaudit -t`.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run `seaudit -t`.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

- **Program** Identifies the name of the program that triggered the event. That is, the program that the accessor used to try to log in. For Privileged Access Manager administration login, this is the module that logged in (selang, Web Service, and so on).

- **AuditFlags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

## Example: Login Event Message

The following audit record was taken from a detailed seaudit output.

```
28 Oct 2008 12:15:01 P LOGIN root 49047159:0000034b 59 2 _CRONJOB_ SBIN_CRON
Event: Login event
Status: Permitted
UserName: root
Terminal: _CRONJOB_
Program: SBIN_CRON
Date: 28 Oct 2008
Time: 12:15
```

```

Details: Resource UACC check
SessionID: 49047159:0000034b
AuditFlags: AC database user

```

This audit record indicates that on October 28th 2008, at 12:15:01 user root logged in to the protected host from terminal `_CRONJOB_` and ran a `SBIN_CRON` program. Privileged Access Manager permitted the operation because the resource's default access permissions permit this action (authorization stage code 59Resource UACC check). The product logged this event because the accessor's audit mode specifies that this event should be logged (reason code 2User audit mode requires logging).

## Logout Event

### Valid on UNIX

Logout events describe an attempt to log out from Privileged Access Manager or a Privileged Access Manager protected host.

#### NOTE

Logout events are only supported on UNIX. Privileged Access Manager does not actually intercept logout. Instead, it assumes logout occurs when the last process for the session terminates.

Audit records in this event have the following format:

```
Date Time Status Event UserName SessionID Details Reason Terminal AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

#### NOTE

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

#### NOTE

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates that a user logout occurred.

**Value:** O (Logout)

- **Event**

Identifies the type of event this record belongs to.

#### NOTE

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **UserName**

Identifies the name of the accessor that performed the action that triggered this event.

- **SessionID**

Identifies the accessor's session ID.

#### NOTE

By default this field does not appear in a non-detailed seaudit output. To display this field in a non-detailed seaudit output, specify the `-sessionid` option in the seaudit command.

- **Details**



Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run `seaudit -t`.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run `seaudit -t`.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

- **AuditFlags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

### Example: Logout Event Message

The following audit record was taken from a detailed seaudit output.

```
29 Jan 2009 17:23:33 O LOGOUT root 49 2 computer.com
Event type: Logout
Status: Logout
User name: root
Terminal: computer.com
Date: 29 Jan 2009
Time: 17:23
Details: Logout detected after last process terminated
Audit flags: AC database user
```

This audit record indicates that on January 29th 2009, Privileged Access Manager detected that the last session process for the user root working on the remote terminal computer.com has closed, and so assumes that the user logged out of the system (authorization stage code 49Logout detected after last process terminated).

### Login Account Enabled Event

#### Valid on UNIX

Login account enabled events describe events where serevu enables a user log in.

Audit records in this event have the following format:

```
Date Time Status Event UserName Details Reason Terminal Program AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates serevu enabled user login.

**Value:** E (Login enabled)

- **Event**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **UserName**

Identifies the name of the accessor that performed the action that triggered this event.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

- **Program**

Identifies the name of the program that triggered the event.

- **AuditFlags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

### Example: Login Account Enabled Event Message

The following audit record was taken from a detailed seaudit output.

```
13 Jan 2009 17:05:00 E LOGINENABLE test1 0 5 computer.com serevu
Event type: Login account enabled
Status: Login enabled
User name: test1
Details: Stage code 0
```

```

Terminal: computer.com
Date: 13 Jan 2009
Time: 17:05
Program: serevu
Audit flags: AC database userLogin account disable -

```

This audit record indicates that on January 13th 2009, the serevu daemon enabled user test1 to log in from the terminal computer.com. Privileged Access Manager logged this event because the serevu daemon requested the audit (reason code 5CA Privileged Access Manager serevu utility requested auditing).

## Login Account Disabled Event

### Valid on UNIX

Login account disabled events describe events where serevu disables a user log in.

Audit records in this event have the following format:

```
Date Time Status Event UserName Details Reason Terminal Program AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates serevu disabled user login.

**Value:** I (Login disabled)

- **Event**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **UserName**

Identifies the name of the accessor that performed the action that triggered this event.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

- **Program**

Identifies the name of the program that triggered the event.

- **AuditFlags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

**Example: Login Account Disabled Event Message**

The following audit record was taken from a detailed seaudit output.

```
13 Jan 2009 16:53:26 I LOGINDISABLE test1          0  5 computer.com      serevu
Event type: Login account disable
Status: Login disabled
User name: test1
Terminal: computer.com
Date: 13 Jan 2009
Time: 16:53
Program: serevu
Details: Stage code 0
User Logon Session ID: 496b629c:00000003
Audit flags: AC database user
```

This audit record indicates that on January 13th 2009, the serevu daemon prevented user test1 from logging in from the terminal computer.com. Privileged Access Manager logged this event because the serevu daemon requested the audit (reason code 5CA Privileged Access Manager serevu utility requested auditing).

**Password Attempt Event****Valid on UNIX**

Password attempt events describe an attempt by an accessor to log in with an incorrect password.

Audit records in this event have the following format:

```
Date Time Status Event UserName Details Reason Terminal Program AuditFlags
```

- **Date**

Identifies the date that the event occurred.

**Format:** DD MMM YYYY

**Note:** Privileged Access Manager Endpoint Management formats the date display according to your computer settings.

- **Time**

Identifies the time that the event occurred.

**Format:** HH:MM:SS

**Note:** Privileged Access Manager Endpoint Management formats the time display according to your computer settings.

- **Status**  
Indicates an incorrect password attempt.  
**Value:** A (Password attempt)
- **Event**  
Identifies the type of event this record belongs to.  
**Note:** Privileged Access Manager Endpoint Management refers to this field simply as *Event*.
- **UserName**  
Identifies the name of the accessor that performed the action that triggered this event.
- **Details**  
Indicates at which stage Privileged Access Manager decided what action to take for this event.  
**Note:** The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message that is associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.
- **Reason**  
Indicates the reason that Privileged Access Manager wrote an audit record.  
**Note:** This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record that you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.
- **Terminal**  
Identifies the name of the terminal that the accessor used to connect to the host.
- **Program**  
Identifies the name of the program that triggered the event.
- **AuditFlags**  
Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.  
**Note:** If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

#### Example: Password Attempt Event Message

The following audit record was taken from a detailed seaudit output.

```
13 Jan YYYY
16:21:12 A LOGIN          admin          17  8 localhost.localdomain login

Event: Password attempt

Status: Password attempt

UserName: admin

Terminal: localhost.localdomain

Date: 13 Jan YYYY

Time: 16:21

Program: login
```

Details: Attempt rejected by the native environment

User Logon Session ID: 525f8d59:0000010a

AuditFlags: AC database user

This audit record indicates that on January 13, YYYY, the user admin attempted to change the account password. The attempt was rejected by the native environment because of a login failure (authorization stage code 17 attempt rejected by the native environment). The pam\_seos module logged this event (reason code 8 pam support UNIX failed login).

## Resource Access Event

Resource access events describe access attempts to resources, for example, FILE, TERMINAL, PROGRAM, and more. The audit record data in this event can appear in other records, for example, a LOGIN event when an accessor attempts to access a TERMINAL resource. Although the event record in this case is of the LOGIN type, the audit record data that appears in the record is one of the Resource Access Event messages.

Audit records in this event have the following format:

```
Date Time Status Class UserName SessionID Access Details Reason Resource Program Terminal EffectiveUserName
AuditFlags
```

### NOTE

In UNIX or Linux, the *AuditFlags* parameter precedes the *EffectiveUserName* parameter

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

### NOTE

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

### NOTE

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Values:** Can be one of:

- D (Denied)Denied the event because of insufficient authorization.
- P (Permitted)Permitted the event.
- W (Warning)Permitted the event because Warning mode is set although the access request violates an access rule.
- N (Notify)Permitted the event and notifies that an attempt to access a permitted resource occurred.
- F (Failed)Permitted, but the Operating System command failed.

- **Class**

Identifies the class that the resource being accessed belongs to.

- **User Name**

Identifies the name of the accessor that performed the action that triggered this event.

- **User Logon Session ID**

Identifies the accessor's session ID.

**NOTE**

By default this field does not appear in a non-detailed seaudit output. To display this field in a non-detailed seaudit output, specify the `-sessionid` option in the seaudit command.

- **Access**

Identifies the type of attempted access that triggered this event.

**Example:** Read

**NOTE**

Access values depend on the class the intercepted resource belongs to. For more information on the access authority for each class, see the *selang Reference Guide*.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run `seaudit -t`.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run `seaudit -t`.

- **Resource**

Identifies the name of the actual resource that is being accessed or updated.

- **Program**

Identifies the name of the program that triggered the event. That is, the program that the accessor used to try to access the resource.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host. (UNIX and Windows.)

- **Effective User Name**

Identifies the name of the native OS effective user that triggered this event. This is different from the user name if the user substitutes (surrogates) to a different user or runs a `setuid` program.

- **Audit Flags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

### Example: Resource Access Event Message

The following audit record is taken from a detailed seaudit output.

```
18 Nov 2008 15:23:56 D FILE          admabc  4922ae61:00000132 Read      69   3 /tmp/one          /usr/
local/bin/tcsh localhost      admabc
Event type: Resource access
Status: Denied
Class: FILE
Resource: /tmp/one
Access: Read
User name: admabc
```

```

Terminal: localhost
Program: /usr/local/bin/tcsh
Date: 18 Nov 2008
Time: 15:23
Details: No Step that allowed access
User Logon Session ID: 4922ae61:00000132
Audit flags: AC database user
Effective user name: admabc

```

This audit record indicates that on November 18th 2008, at 15:23:56 the user admabc used UNIX tcsh shell program from the local computer to try and read the protected /tmp/one file resource. Privileged Access Manager denied the operation because there are no rules in the database that authorize this type of access (authorization stage code 69No step that allowed access). Privileged Access Manager logged this event because the resource's audit mode specifies that this event should be logged (reason code 3Resource audit mode required logging).

## Untrust Message Event

Untrust events describe warning messages that the Privileged Access Manager Watchdog generates for events.

Audit records in this event have the following format:

```
Date Time Status Class Module Details MessageID/errno File
```

- **Date**  
Identifies the date that the event occurred.  
**Format:** DD MMM YYYY  
**Note:** Privileged Access Manager Endpoint Management formats the date display according to your computer settings.
- **Time**  
Identifies the time that the event occurred.  
**Format:** HH:MM:SS  
**Note:** Privileged Access Manager Endpoint Management formats the time display according to your computer settings.
- **Status**  
Indicates untrust occurred.  
**Value:** U (Untrust)
- **Class**  
Identifies the Privileged Access Manager class that the resource that triggered the Watchdog message belongs to.  
**Values:** PROGRAM or SECFILE
- **Module Name**  
Displays the name of the Privileged Access Manager Watchdog.  
**Value:** seoswd
- **Details**  
Indicates why the untrust event occurred.  
**Note:** The audit record that you see in a non-detailed seaudit output displays a number in this field. This number is known as the untrust reason code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message that is associated with the untrust reason code. For a complete list of password quality codes, run seaudit -t.
- **Message ID**  
(UNIX only) Indicates the reason Privileged Access Manager untrusted the PROGRAM or SECFILE.  
**Note:** The audit record that you see in a non-detailed seaudit output displays a number in this field. This number is known as the status code and does not show in a detailed output or in Privileged Access Manager Endpoint



Management. To understand the status code, run `seaudit -Stat untrust_code`. This field displays only if the authorization stage code is 1. In all other cases, the `errno` field displays instead.

- **errno**

Indicates the return value of the `errno` variable (the error code for the error condition).

**Values:** can be one of:

**0**No error. This value is returned only if the authorization stage code is 1. In this case, the `errno` field is not displayed and the Message ID field displays instead.

*errno*A non-zero integer that is the error.

**Note:** To find out the meaning for the error, on UNIX, see `/usr/include/errno.h` or `/usr/include/sys/errno.h` file on the local computer. On Windows, enter the following command on the local computer: `net helpmsg errno`

- **File**

Identifies the full pathname of the protected resource that triggered the Watchdog message.

### Example: Untrust Message Event Message

The following audit record was taken from a detailed `seaudit` output.

```
18 Nov YYYY 14:01:18 U PROGRAM      seoswd                1 11776 /tmp/testsuiteid

Event type: Untrust message

Class: PROGRAM

Module name: seoswd

Message ID: 11776

Date: 18 Nov YYYY

Time: 14:01

File: /tmp/testsuiteid

Details: Stat information changed on file system

Audit flags: AC database user
```

This audit record indicates that on November 15 of the specified year, the Watchdog marked the program `/tmp/testsuiteid` as untrusted (U). The program was untrusted because the file status information was modified (untrust reason code 1File information changed on file system).

### Example: Use `seaudit -Stat` to See Why a Program Was Untrusted (UNIX)

The following `seaudit -Stat` output shows you how you can get more detailed information about the Watchdog message ID that an audit record mentions.

```
# seaudit -Stat 11776

CA PAMSC seaudit v12.01.00.45 - Audit log lister

Copyright (c) YYYY CA. All rights reserved.
```

The MODE of the file was changed

The INODE of the file was changed

The SIZE of the file was changed

The MTIME of the file was changed

Running the `seaduit -Stat` command with the message ID, displays a list of changes to the file. In this example, the MODE, INODE, SIZE, and MTIME of the file changed. As a result Privileged Access Manager marked this file as an untrusted file.

## Inbound Network Connection Event

Inbound network connection events indicate incoming traffic to the protected host. Inbound network events are audited in two forms (according to the class activation in the local database). Both audit event types contain identical information but in different view. For example, one audit event contains HOST as the class name while the other event displays TCP as the class name.

Audit records in this event have the following format:

```
Date Time Status Event Service Details Reason Host Program
```

- **Date**  
Identifies the date the event occurred.  
**Format:** DD MMM YYYY  
  
**NOTE**  
Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.
- **Time**  
Identifies the time the event occurred.  
**Format:** HH:MM:SS  
  
**NOTE**  
Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.
- **Status**  
Indicates the return code for the event.  
**Values:** Can be one of:
  - D (Denied)Denied the event because of insufficient authorization.
  - P (Permitted)Permitted the event.
  - W (Warning)Permitted the event because Warning mode is set although the access request violates an access rule.
- **Event Type**  
Identifies the type of event this record belongs to.  
  
**NOTE**  
Privileged Access Manager Endpoint Management refers to this field simply as *Event*.
- **Service**

Identifies the name of the service that the connection used.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Host name**

Identifies the name of the host the network traffic originated from.

- **Program**

(UNIX only) Identifies the name of the program the accessor is attempting to run.

### Example: Inbound Network Connection Event Message

The following audit record was taken from a detailed seaudit output.

```
17 Nov 2008 12:22:04 D HOST          telnet          173  3 computer.org.com      /usr/sbin/inetd
Event type: Inbound network connection
Status: Denied
Host name: computer.org.com
Service: telnet
Program: /usr/sbin/inetd/
Date: 17 Nov 2008
Time: 12:22
Details: HOST entry day & time restrictions
Audit flags: AC database user
```

This audit record indicates that on November 17th 2008, an accessor attempting to access the host computer.org.com using the telnet service to run the inetd program was denied due to day and time restrictions imposed on the protected host (authorization stage code 173HOST entry day & time restrictions). Privileged Access Manager logged this event because the resource's audit mode specifies that this event should be logged (reason code 3Resource audit mode required logging).

### Outbound Network Connection Event

Outbound network connection events indicate outbound traffic to the protected host. Outbound network events are audited in two forms (according to the class activation in the local database). Both audit event types contain identical information but in different view. For example, one audit event contains HOST as the class name while the other event displays TCP as the class name.

Audit records in this event have the following format:

```
DateTimeStatusClassServiceUserNameDetailsReasonHostProgramTerminal AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Values:** Can be one of:

- D (Denied) Denied the event because of insufficient authorization.
- P (Permitted) Permitted the event.
- W (Warning) Permitted the event because Warning mode is set although the access request violates an access rule.

- **Class**

Identifies the name of the class.

- **Service**

Identifies the name of the service that the connection used.

- **User Name**

Identifies the name of the accessor that performed the action that triggered this event.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Host name**

Identifies the name of the target host.

- **Program**

Identifies the name of the program that triggered the event.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

- **User Logon Session ID**

Identifies the accessor's session ID.

**NOTE**

By default this field does not appear in a non-detailed seaudit output. To display this field in a non-detailed seaudit output, specify the -sessionid option in the seaudit command. The user logon session ID field is added only to events that were generated as a result of TCP or CONNECT class definitions.

- **Audit Flags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

**Example: Outbound Network Connection Event Message**

The following audit record was taken from a detailed seaudit output.

```
21 Jan 2009 15:37:43 D TCP          telnet      root        408 2 computer.org /usr/bin/telnet computer.com

Event type: Outbound network connection
Status: Denied
Host name: computer.org
Service:telnet
Program: /usr/bin/telnet
User name: Administrator
Terminal: computer.com
User name: root
Date: 21 Jan 2009
Time: 15:37:43
Details: Default access of TCP service
User Logon Session ID: 4977248c:0000012a5248
Audit flags: AC database user
```

This audit record indicates that on January 21st, 2009, the administrator opened an outgoing connection from the terminal computer.org to the computer named computer.com via the telnet service. Privileged Access Manager denied this operation because of the defaccess property of the TCP record. (authorization stage code 408Default of TCP service). Privileged Access Manager logged this event because the AUDIT\_MODE property for the accessor matches the record's result. (reason code 2User audit mode requires logging).

**Security Database Administration Event**

Security database administration events describe actions performed by a Privileged Access Manager administrator or a sub-administrator with appropriate privileges that were intercepted by the product.

Audit records in the event have the following format:

```
Date Time Status Event Class Admin Details Reason Object TerminalCommand AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Values:** Can be one of:

- D (Denied) Denied the event because of insufficient authorization.
- S (Success) Permitted the event.
- F (Failed) Failed the event.

- **Event Type**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **Class**

Identifies the class that the resource being administered belongs to.

- **Administrator**

Identifies the name of the administrative user that executed the selang command.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Object**

Identifies the name of the resource that is being administrated.

- **Terminal**

Identifies the name of the terminal that the accessor used to connect to the host.

**NOTE**

If the command originated from a parent policy model, this field displays the fully qualified PMD name.

- **Command**

Displays the selang command that the user executed.

- **Audit Flags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

- **Command type**

Identifies the type of the database administration command that this event describes.

Values can be one of:

- **Add user:** For newusr command
- **Add group:** For newgrp command
- **Add resource:** For newres or newfile commands
- **Modify user:** For chusr command
- **Modify group:** For chgrp command
- **Modify group membership:** For join command
- **Modify resource:** For chres command
- **Modify resource access:** For authorize command
- **Remove user:** For rmusr command
- **Remove group:** For rmgrp command
- **Remove resource:** For rmres or rmfile commands
- **Set options:** For setoptions command
- **Add/Modify user:** For editusr command
- **Add/Modify group:** For editgrp command
- **Add/Modify resource:** For editres or editfile commands
- **Administrative command:** For other commands

### Example: Security Database Administration Event Message

The following audit record was taken from a detailed seaudit output.

```
05 Nov 2008 15:45:12 S UPDATE      FILE      DOMAIN_NAME\computer 305  0 dfdok      computer.com cr file
dfdok defacc(r)
Event type: Security database administration
Command type: Modify resource
Status: Successful
Administrator: DOMAIN_NAME\computer
Class: FILE
Object: dfdok
Terminal: computer.com
Date: 05 Nov 2008
Time: 15:45
Details: Command successful for ADMIN user.
Command: cr file dfdok defacc(r)
Audit flags: AC database user
```

This audit record indicates that on November 5th 2008, Privileged Access Manager denied access from an administrator attempting to update a file by executing the command `cr file dfdok defacc(r)` on the protected host logging from the terminal `computer.com` (authorization stage code 305Command allowed for ADMIN user).

### Startup Event

Privileged Access Manager startup events describe the startup sequence of Privileged Access Manager services (Windows) or daemons (UNIX).

Audit records in the event have the following format:

```
DateTime M Event Service
```

- **Date**  
Identifies the date the event occurred.  
**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Event Type**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **Service**

seosd - the main Privileged Access Manager daemon or service. The seosd daemon or service controls the start up and shutdown sequences of the product.

**Example: Daemon Start Event Message (UNIX)**

The following audit record was taken from a detailed seaudit output.

```
02 Nov 2008 15:41:06 M START                                seoswd
Event type: Daemon start
Daemon: seoswd
Date: 02 Nov 2008
Time: 15:41
Audit flags: AC database user
```

This audit record indicates that on November 2nd 2008 the seoswd Watchdog started.

**Example: Engine Service Start Event Message (Windows)**

The following audit record was taken from a detailed seaudit output.

```
02 Nov 2008 15:34:48 M START                                seosd
Event type: Engine service start
Engine service: seosd
Date: 02 Nov 2008
Time: 15:34
Audit flags: AC database user
```

This audit record indicates that on November 2nd 2008, the seosd service engine, responsible for starting up Privileged Access Manager, started.

**Shutdown Event**

Privileged Access Manager shutdown events describe shutdown processes that are performed by an administrator or sub-administrator user with privileges to shutdown the system.

Audit records in this event have the following format:

```
Date Time M Event UserName SessionID Details Service AuditFlags
```



- **Date**  
Identifies the date that the event occurred.  
**Format:** DD MMM YYYY  
**Note:** Privileged Access Manager Endpoint Management formats the date display according to your computer settings.
- **Time**  
Identifies the time that the event occurred.  
**Format:** HH:MM:SS  
**Note:** Privileged Access Manager Endpoint Management formats the time display according to your computer settings.
- **Event Type**  
Identifies the type of event this record belongs to.  
**Note:** Privileged Access Manager Endpoint Management refers to this field simply as *Event*.
- **User Name**  
Identifies the name of the accessor that performed the action that triggered this event.
- **User Logon Session ID**  
Identifies the accessor's session ID.  
**Note:** By default this field does not appear in a non-detailed seaudit output. To display this field in a non-detailed seaudit output, specify the -sessionid option in the seaudit command.
- **Details**  
Indicates at which stage Privileged Access Manager decided what action to take for this event.  
**Note:** The audit record that you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message that is associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.
- **Daemon (UNIX) / Engine service (Windows)**  
Identifies the name of the Privileged Access Manager daemon (UNIX) or service (Windows) that was shut down.  
**Value:** seosd (the Privileged Access Manager Engine).
- **Audit Flags**  
Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.  
**Note:** If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

#### Example: Shutdown Event Message on UNIX

The following audit record was taken from a detailed seaudit output.

```
24 Sep YYYY 15:40:46 M SHUTDOWN      root      452 seosd
```

```
Event type: Daemon shutdown
```

```
User name: root
```

```
Daemon: seosd
```

```
Date: 24 Sep YYYY
```

```
Time: 15:40:46
```

```
Details: User is ADMIN or SPECIAL
```

```
User Logon Session ID: 48da26ce:00000142
```

Audit flags: CA PAMSC database user

This audit record indicates that on September 24th of the specified year, the user root who was attempting to shutdown Privileged Access Manager was permitted to do so because the user has the ADMIN attribute (authorization stage code 452User is ADMIN or SPECIAL).

### Example: Shutdown Event Message on Windows

The following audit record was taken from a detailed seaudit output.

```
23 Dec YYYY 12:56:20 D SHUTDOWN      tst002                460 seosd
```

Event type: Engine service shutdown

User name: tst002

Engine service: seosd

Date: 10 Feb 2009

Time: 12:56

Details: User is not allowed to shutdown CA PAMSC

User Logon Session ID: 00000000:04c240d5

Audit flags: AC database user

This audit record indicates that on December 23rd of the specified year, the Privileged Access Manager shut down was denied because the user tst002 is not allowed to shutdown the product (authorization stage code 460User is not allowed to shutdown Privileged Access Manager).

### Password Verification Event

Password verification event type messages indicate that a user failed to change his account's password.

Audit records in this event have the following format:

```
DateTime Status EventUserName DetailsReason AuditFlags
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Value:** F (Failed)Failed to change the account password.

- **Event Type**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **User Name**

Identifies the name of the user to which the password attempt was applied.

- **Details**

Indicates why the password change attempt failed.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the password quality code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the password quality code. For a complete list of password quality codes, run seaudit -t.

- **Reason**

Indicates the reason that Privileged Access Manager wrote an audit record.

**NOTE**

This field does not display in a detailed seaudit output or in Privileged Access Manager Endpoint Management. The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the reason code. For a complete list of reason codes, run seaudit -t.

- **Audit Flags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

**Example: Password Verification Event Message**

The following audit record was taken from a detailed seaudit output.

```
02 Dec 2008 10:23:47 F PASSWORD      test1          1 10
Event type: Password verification
Status: Failed
User name: test1
Details: Password too short
Audit flags: AC database user
```

This audit record indicates that on December 2nd 2008, the user attempting to change his account password was denied because the password did not meet the minimum required number of characters, as defined by the password policy (authorization stage code 1Password too short). Privileged Access Manager logged this event message according to an explicit request (reason code 10An explicit request to log the operation was received).

**Trace Message On a User**

Trace messages on user events describe an attempt to open, run, or use a protected resource.

Audit records in this event have the following format for Windows:

```
Date Time Status Event UserNameSessionID RealUID RealUsername Class Resource DetailsAuditFlags Trace
```

Audit records in this event have the following format for UNIX:

```
Date Time Status Event UserNameSessionID EffectiveUsername RealUsername Class Resource DetailsAuditFlags
Trace
```

- **Date**

Identifies the date the event occurred.

**Format:** DD MMM YYYY

**NOTE**

Privileged Access Manager Endpoint Management formats the date display according to your computer's settings.

- **Time**

Identifies the time the event occurred.

**Format:** HH:MM:SS

**NOTE**

Privileged Access Manager Endpoint Management formats the time display according to your computer's settings.

- **Status**

Indicates the return code for the event.

**Values:** Can be one of:

- D (Denied)Denied the event because of insufficient authorization.
- P (Permitted)Permitted the event.
- W (Warning)Permitted the event because Warning mode is set although the access request violates an access rule.

**NOTE**

In a detailed seaudit output this field displays the trace information.

- **Event Type**

Identifies the type of event this record belongs to.

**NOTE**

Privileged Access Manager Endpoint Management refers to this field simply as *Event*.

- **User Name**

Identifies the name of the accessor that performed the action that triggered this event.

- **User Logon Session ID**

Identifies the accessor's session ID.

- **Real User ID**

Identifies the user ID of the user who invoked the process.

**Note:** (UNIX) This field does not appear in non-detailed seaudit output.

- **Real user name**

Identifies the name of the user performing the traced action.

- **Effective user ID**

(UNIX only) Indicates the ID of the native OS effective user ID.

**Note:** This field does not appear in non-detailed seaudit output.

- **Effective User Name**

Identifies the name of the native OS effective user that triggered this event. This is different from the user name if the user substitutes (surrogates) to a different user or runs a setuid program.

- **Class**

Identifies the class that the resource being accessed belongs to.

- **Resource**

Identifies the name of the actual resource that is being accessed or updated.

- **Details**

Indicates at which stage Privileged Access Manager decided what action to take for this event.

**NOTE**

The audit record you see in a non-detailed seaudit output displays a number in this field. This number is known as the authorization stage code. In a detailed output or in Privileged Access Manager Endpoint Management, the audit record displays the message associated with the authorization stage code. For a complete list of stage codes, run seaudit -t.

- **Trace information**

Displays the trace detail information including the class, resource, and action that was performed on that resource or the result of that action.

- **Audit Flags**

Indicates whether the accessor is internal (Privileged Access Manager database user) or an enterprise user.

**NOTE**

If the accessor is an enterprise user, the audit record you see in a non-detailed seaudit output displays the string "(OS user)" in this field. Otherwise, this field remains empty.

### Example: Trace Message On a User Event Message on UNIX

The following audit record was taken from a detailed seaudit output.

```
03 Nov 2008 10:38:47 P TRACE      root      490dadd:00000140 john      root      FILE      /
home/jon/file.txt  55 FILE    > Result: 'P' [stage=55 gstag=55 ACEEH=8   rv=0 (/home/john/file.txt
Event type: Trace message on a user
Date: 03 Nov 2008
Time: 10:38
Details: Resource ACL check
Trace information: FILE    > Result: 'P' [stage=55 gstag=55 ACEEH=8   rv=0 (/home/john/file.txt
Class: FILE
Resource: /home/admin/file.txt
User name: root
Real user ID: 108
Real user name: john
Effective user ID: 108
Effective user name: root
User Logon Session ID: 490dadd:00000140
Audit flags: AC database user
```

This audit record indicates that on November 3rd 2008, a trace message was logged due to an administrator attempt to access a resource belonging to a FILE class. The administrator was permitted to access according to the ACL of the accessed resource (authorization stage code 55Resource ACL check).

### Example: Trace Message On a User Event Message on Windows

The following audit record was taken from a detailed seaudit output.

```
10 Nov 2008 10:14:53 P TRACE      MACHINE\Administrator 00000000:172ef9ef MACHINE\john MACHINE\john
WINSERVICE _default    1059 WINSERVICE > (C:\WINDOWS\system32\services.exe) Result: 'P' [stage=1059
gstag=1059 ACEEH=6   rv=0x0 (WebClient)]      Why? Default record universal access check
Event type: Trace message on a user
Date: 10 Nov 2008
Time: 10:14
Details: Default record universal access check
Trace information: WINSERVICE > (C:\WINDOWS\system32\services.exe) Result: 'P' [stage=1059 gstag=1059 ACEEH=6
rv=0x0 (WebClient)]      Why? Default record universal access check
```

```

Class: WINSERVICE
Resource: _default
User name: MACHINE\Administrator
Real user name: MACHINE\john
User Logon Session ID: 00000000:172ef9ef
Audit flags:AC database user

```

This audit record indicates that on November 10th 2008, a trace message was triggered due to an administrator attempting to access the resource \_default belonging to the WINSERVICE class. The administrator was permitted access because of a record universal access check (authorization stage code 1059Default record universal access check).

## Audit Records

Each record in the audit log contains data that is arranged in columns. Two columns (date and time stamps) are common to all types of records. The remaining columns and the data they contain depend on the type of event that triggered the creation of the audit record.

### NOTE

The order, number, and content of columns that you see for an audit log record depend on the method you choose to view the audit log. Some fields do not display in Privileged Access Manager Endpoint Management, seaudit output, or the detailed seaudit output. Also, if you use the seaudit utility, the options you specify may also determine the number, order, and content of the columns.

## How To Identify the Event Type of an Audit Record

To understand the content of an audit record, you must first identify the event type of the audit record. This is because the data the record contains depends on the type of event that triggered the creation of the audit record.

### NOTE

The order, number, and content of columns that you see for an audit log record depend on the method you choose to view the audit log. Some fields do not display in Privileged Access Manager Endpoint Management, seaudit output, or the detailed seaudit output. Also, if you use the seaudit utility, the options you specify may also determine the number, order, and content of the columns.

To identify the event type of an audit record:

- If you are viewing audit records in Privileged Access Manager Endpoint Management, the event type the audit record belongs to displays in the first column of the Audit Records Result pane.  
To display more information about the audit record, click the link audit event type in the first column.
- If you are viewing audit records in seaudit output, you need to display the detailed output (-detail option) to see the event type.

Once you identify the event type, you can go on to interpret the rest of the message detail.

### Example: Audit Records in CA Privileged Access Manager Endpoint Management

The following image shows you how Endpoint Management presents audit events:

Audit Records Result							
These are the audit records filter by: 'timed'. Last update: 12/19/08 7:26 PM							
Show: 10 Events / Page							
Event	Date	Status	Class	User Name	Object/Resource	Terminal	Program
Security DB Admin	Dec 19, 2008 6:28:18 PM GMT+11:00	Success	TERMINAL	TM123VW-AC\Administrator	TM123VW-AC-SC1.com.com	TM123VW-AC	
Login Event	Dec 19, 2008 6:28:18 PM GMT+11:00	Permitted		TM123VW-AC\Administrator		TM123VW-AC	selang
Security DB Admin	Dec 19, 2008 4:47:16 PM GMT+11:00	Success	GROUP	TM123VW-AC\Administrator	test	TM123VW-AC	
Resource Access	Dec 19, 2008 4:47:12 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe
Resource Access	Dec 19, 2008 4:47:07 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe
Resource Access	Dec 19, 2008 4:47:02 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe
Resource Access	Dec 19, 2008 4:46:57 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe
Login Event	Dec 19, 2008 4:46:53 PM GMT+11:00	Permitted		TM123VW-AC\Administrator		TM123VW-AC	C:\WINDOWS\system32\lsass.exe
Resource Access	Dec 19, 2008 4:46:52 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe
Resource Access	Dec 19, 2008 4:46:47 PM GMT+11:00	Permitted	WINSERVICE	TM123VW-AC\Administrator	VMTools	TM123VW-AC	C:\WINDOWS\system32\services.exe

### Example: Audit Records in Default seaudit Output

The following snippet of a seaudit output shows you how the seaudit utility presents audit events by default:

```

19 Dec 2008 16:46:47 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:52 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:53 P LOGIN          TM123VM-AC\Administrator  55    2 TM123VM-AC        C:\WINDOWS
\system32\lsass.exe
19 Dec 2008 16:46:57 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:02 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:07 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:12 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:16 S UPDATE        GROUP      TM123VM-AC\Administrator  336   0 test             TM123VM-AC egtest
audit-
19 Dec 2008 18:28:18 P LOGIN          TM123VM-AC\Administrator  55   10 TM123VM-AC        selang
19 Dec 2008 18:28:18 S UPDATE        TERMINAL   TM123VM-AC\Administrator  305   0 TM123VM-AC-SC1.ca.com TM123VM-
AC er terminal TM123VM-AC-SC1.ca.com

```

The detailed seaudit output for the first message above is as follows:

```

19 Dec 2008 16:46:47 P WINSERVICE    TM123VM-AC\Administrator Read      1059  2 VMTools          C:\WINDOWS
\system32\services.exe TW852VM-AC
Event type: Resource access
Status: Permitted
Class: WINSERVICE
Resource: VMTools
Access: Read
User name: TM123VM-AC\Administrator
User Logon Session ID: 00000000:05647d29
Terminal: TM123VM-AC
Program: C:\WINDOWS\system32\services.exe
Date: 19 Dec 2008
Time: 16:46
Details: Default record universal access check
Audit flags: AC database user

```

## Authorization Stage Codes for Inbound Network Connection Events

Authorization stage codes for inbound network connection events describe at which stage Privileged Access Manager decided what action to take for the incoming network connection event.

Authorization Stage Code	Indicates
150 Check Class Table	The class could not be found in the Privileged Access Manager database. Privileged Access Manager may write this message to the audit log if there is a problem in the product database. To correct this problem, use the dbmgr utility to rebuild the CA product database. <b>Important!</b> Use the dbmgr utility only with the guidance of support personnel during problem resolution. For assistance, contact CA Support at <a href="http://ca.com/support">http://ca.com/support</a> .
153 HOST entry asterisk in inetacl	Indicates that Privileged Access Manager permitted or denied a connection from a protected host, because the host INETACL contains an asterisk (*). An asterisk specifies any sequence of zero or more characters and therefore matches all services when used in INETACL.
156 HOST entry inetacl	Privileged Access Manager permitted or denied a connection from the protected host, because the host INETACL lists the connection service.
157 HOST Class UACC	Privileged Access Manager permitted or denied a connection from the protected host, because of the default access authority value defined for the host UACC class.
159 HOST entry service range ACL	Privileged Access Manager permitted or denied a connection from the protected host, because the connection service is within the host INETACL range.
163 No rule granting access to service	Privileged Access Manager denied a connection from the host, because it did not find a rule permitting access. Check the HOST class access rules for that host.
164 HOST group inetacl	Privileged Access Manager permitted or denied a connection from the protected host, because the GHOST object's INETCAL lists the connection service.
165 HOST group service range ACL	Privileged Access Manager permitted or denied a connection from the protected host, that is a member of the GHOST host group object, because the connection service is within the host group's INETACL range.
166 HOST group asterisk in inetacl	Privileged Access Manager permitted or denied a connection from a protected host that is a member of the GHOST host group object, because the host group's INETACL contains an asterisk (*). An asterisk specifies any sequence of zero or more characters and therefore matches all services when used in INETACL.
167 HOSTNET (network or IP mask match) inetacl	Privileged Access Manager permitted or denied a connection from the protected host, because the HOSTNET record INETACL lists the connection service.
168 HOSTNET (network or IP mask match) service range	Privileged Access Manager permitted or denied a connection from the protected host, because the connection service is within the HOSTNET record INETACL range.



169 HOSTNET (network or IP mask match) inetacl asterisk	Privileged Access Manager permitted or denied a connection from a protected host, because the HOSTNET record INETACL contains an asterisk (*). An asterisk specifies any sequence of zero or more characters and therefore matches all services when used in INETACL.
170 HOSTNP (hosts name pattern) inetacl	Privileged Access Manager permitted or denied a connection from the protected host, because the HOSTNP record INETACL lists the connection service.
171 HOSTNP (hosts name pattern) service range	Privileged Access Manager permitted or denied a connection from the protected host, because the connection service is within the HOSTNP record INETACL range.
172 HOSTNP (hosts name pattern) inetacl asterisk	Privileged Access Manager permitted or denied a connection from a protected host, because the HOSTNP record INETACL contains an asterisk (*). An asterisk specifies any sequence of zero or more characters and therefore matches all services when used in INETACL.
173 HOST entry day & time restrictions	Privileged Access Manager denied access to a protected host, because the attempted access was outside the day and time restrictions in the HOST record.
174 HOST group day & time restrictions	Privileged Access Manager denied access to a protected host group, because of the day and time restrictions in the GHOST record.
175 HOSTNET (network or IP mask match) day & time restrictions	Privileged Access Manager denied access to a protected host, because of the day and time restrictions in the HOSTNET record.
176 HOSTNP (hosts name pattern) day & time restrictions	Privileged Access Manager denied access to a protected host, because of the day and time restrictions in the HOSTNP record.
177 HOST_default day & time restrictions	Privileged Access Manager denied access to a protected host, because of the day and time restrictions in the HOST_default record.
178 HOST_default inetacl	Privileged Access Manager permitted or denied access to a protected host, because of the values in the HOST_default INETACL.
179 HOST_default service range	Privileged Access Manager permitted or denied access to a protected host, because the connection service is within the HOST_default record INETACL range.
180 HOST_default service asterisk	Privileged Access Manager permitted or denied access to a protected host, because the HOST_default record INETACL contains an asterisk (*). An asterisk specifies any sequence of zero or more characters and therefore matches all services when used in INETACL.
404 HOST entry in TCP service ACL	Privileged Access Manager permitted or denied access from a HOST, because the TCP record ACL lists the HOST.
405 GHOST entry in TCP service ACL	Privileged Access Manager permitted or denied access from a HOST, because the TCP record ACL lists the GHOST of which the HOST is a member.
406 HOSTNET entry in TCP service ACL	Privileged Access Manager permitted or denied access from a HOST, because the TCP record ACL lists the HOSTNET network of which the HOST is a part.
407 HOSTNP entry in TCP service ACL	Privileged Access Manager permitted or denied access from a HOST, because the TCP record ACL lists the HOSTNP set of which the HOST is a part.

## Authorization Stage Codes for Log In and Log Out Events

Authorization stage codes for log in and log out events describe at which stage Privileged Access Manager decided what action to take for the log in or log out event.

Authorization Stage Code	Indicates
2 Fetching user object	A login attempt failed because Privileged Access Manager could not load user information, such as user mode, terminal, or login program. Privileged Access Manager may write this message to the audit log if the database is corrupt or the product did not start correctly.
3 Terminal checking for login terminal source	Privileged Access Manager permitted or denied login according to the <b>TERMINAL</b> class rules.
5 User suspend checking	Privileged Access Manager denied login, because the user account is suspended.
6 User expiration checking	Privileged Access Manager denied login, because the user account is expired, as defined in the user's profile.
7 User day-time checkings	Privileged Access Manager denied login, because the user attempted to log in at a time outside the permitted day and time for the product database.
8 Password validity checkings	<b>Valid on UNIX</b> Privileged Access Manager checked a user's password to ensure it conformed to the password rules. Privileged Access Manager may write this message to the audit log when a login attempt failed because a user's password did not conform to the product's database password rules.
9 User grace login checkings	Privileged Access Manager denied login, because the user account has exhausted its grace login attempts.
10 Password expired with no more grace logins	Privileged Access Manager denied login because the password is expired. The user did not change their password within the password interval limit and no grace count after password expiration is configured, neither in the user's profile group's definition nor in the product's global definitions.
11 Building the user ACEE	Privileged Access Manager successfully generated the ACEE for the user.
12 User inactivity days check	Privileged Access Manager denied login, because the user was inactive for a period that exceeded the permitted inactive interval. The permitted inactive interval is defined in the user's profile or global product settings.
13 Too many logins for user	Privileged Access Manager denied login, because the user has exceeded the maximum allowed number of simultaneous logins from different terminals. The maximum allowed number of simultaneous logins is defined in the 'Maxlogins' properly value in the user's profile or global product settings
14 Active HOLIDAY check	Privileged Access Manager denied login, because the user attempted to log in during the restricted holiday dates. The restricted holiday dates are defined in the <b>HOLIDAY</b> class.

15 Login Application (LOGINAPPL) check	<b>Valid on UNIX</b> Privileged Access Manager denied login, because of the LOGINAPPL class rules.
16 User Groups day-time checking	Privileged Access Manager denied login, because the user attempted to log in at a time outside the permitted day and time for the user or for one of the user's group.
17 Attempt rejected by the native environment	The login attempt failed due to the native environment settings. Logged by Privileged Access Manager PAM module.
18 User without domain restriction	<b>Valid on Windows</b> Privileged Access Manager denied login, because the user did not provide a domain name.
19 No reason to deny – allow login	Privileged Access Manager permitted login, because the login attempt passed all check stages, providing that the login authorization has a TERMINAL object assigned to. Viewing this event stage message may indicate that the login authorization was triggered by a Privileged Access Manager authorization API that does not have the terminal name specified.
20 'Logical' user check	Privileged Access Manager denied login, because the product does not permit 'logical' users (users with the <i>logical</i> property set) to log in.
49 Logout detected after last process terminated	<b>Valid on UNIX</b> Privileged Access Manager detected a user logout event occurring after the last process terminated.

## Authorization Stage Codes for Outbound Network Connection Events

Authorization stage codes for outbound network connection events describe at which stage Privileged Access Manager decided what action to take for the outbound network connection event.

Authorization Stage Code	Indicates
400 _default service in class TCP	Privileged Access Manager permitted or denied access to a protected host, because of the _default object permissions in the TCP record for the connecting service.
401 Class UACC of TCP services	Privileged Access Manager permitted or denied access to a protected host, because of the value of the TCP object in the UACC class.
402 Day and time restrictions on TCP service	Privileged Access Manager denied access to a TCP service, because of the day and time restrictions in the TCP record.
403 ACL read stage of TCP service	Privileged Access Manager permitted or denied access to the TCP service, because of the ACL read property in the TCP record. The product may write this message to the audit log if the database is corrupt.
408 Default access of TCP service	Privileged Access Manager permitted or denied access to the TCP class service, because of the defaccess property of the TCP record.  <b>Note:</b> This event message also applies to incoming TCP events to indicate an inbound connection to the HOST.

409 CACL read stage of TCP service	Privileged Access Manager denied access to the TCP service, because of the CACL read property in the TCP record. The product may write this message to the audit log if the database is corrupt.
410 HOST entry for USER in TCP service CACL	Privileged Access Manager permitted or denied access to a HOST object for a specified USER or XUSER. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
411 GHOST entry for USER in TCP service CACL	Privileged Access Manager permitted or denied access to a GHOST object for a specified USER or XUSER object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
412 HOSTNET entry for USER in TCP service CACL	Privileged Access Manager permitted or denied access to a HOSTNET object for a specified USER or XUSER object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
413 HOSTNP entry for USER in TCP service CACL	Privileged Access Manager permitted or denied access to a HOSTNP object for a specified USER or XUSER object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
414 HOST entry for GROUP in TCP service CACL	Privileged Access Manager permitted or denied access to a HOST object for a specified GROUP or XGROUP object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
415 GHOST entry for GROUP in TCP service CACL	Privileged Access Manager permitted or denied access to a GHOST object for a specified GROUP or XGROUP object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
416 HOSTNET entry for GROUP in TCP service CACL	Privileged Access Manager permitted or denied access to a HOSTNET object for a specified GROUP or XGROUP object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
417 HOSTNP entry for GROUP in TCP service CACL	Privileged Access Manager permitted or denied access to a HOSTNP object for a specified GROUP or XGROUP object. The product used the access rules in the CACL of the TCP service to determine whether to permit or deny access.
418 HOST entry for User '*' in TCP service CACL	Privileged Access Manager permitted or denied access to a HOST for a user, because the HOST record CACL contains an asterisk (*). An asterisk specifies all defined users.
419 GHOST entry for User '*' in TCP service CACL	Privileged Access Manager permitted or denied access to a HOST belonging to GHOST class for a user, because the GHOST record CACL contains an asterisk (*). An asterisk specifies all defined users.
420 HOSTNET entry for User '*' in TCP service	Privileged Access Manager permitted or denied access to a HOSTNET object for a user, because the HOSTNET record CACL contains an asterisk (*). An asterisk specifies all defined users.
421 HOSTNP entry for User '*' in TCP service CACL	Privileged Access Manager permitted or denied access to a HOSTNP object for a user, because the HOSTNP record CACL contains an asterisk (*). An asterisk specifies all defined users.

## Authorization Stage Codes for Password Verification Events

Authorization stage codes for password verification events describe at which stage Privileged Access Manager decided what action to take for the password verification event.

Authorization Stage Code	Indicates
0 Password quality verified	The user successfully changed their password, and that the new password meets all of the password quality rules.
1 Password too short	The password change failed, because the length of the new password does not comply with the password policy for minimum password length.
2 Password contains user name	The password change failed, because the new password contains the user's user name.
3 Too few lowercase letters in password	The password change failed, because the new password does not contain enough lower case letters according to the minimum defined in the password policy.
4 Too few capital letters in password	The password change failed, because the new password does not contain enough capital letters according to the minimum defined in the password policy.
5 Too few numeric characters in password	The password change failed, because the new password does not contain enough numeric characters according to the minimum defined in the password policy.
6 Too few other characters in password	The password change failed, because the new password does not contain enough other characters according to the minimum defined in the password policy.
7 Too many repetitions of same char in password	The password change failed, because the new password contains too many repeating characters according to the maximum defined in the password policy.
8 Same as current password	The password change failed, because the new password is the same as the current password. You should select a password that you have not used before.
9 Password previously used. Select a different password	The password change failed, because the new password was previously used. You should select a password that you have not used before.
10 Too few alphabetic characters in password	The password change failed, because the new password does not contain enough alphabetic characters according to the minimum defined in the password policy.
11 Too few alphanumeric characters in password	The password change failed, because the new password does not contain enough alphanumeric characters according to the minimum defined in the password policy.
12 Password was changed recently, cannot be changed again at this time	The password change failed, because the password was recently changed and cannot be changed at this time. You should change the password only after the minimal password age period has passed according to the minimum defined in the password policy.
13 Password is contained by a previous password or vice versa	The password change failed, because the new password contains a previous password or is part of a previous password. You should ensure that the new password does not contain a previous password, and is not part of a previous password.

14 Password contains previous password pattern	The password change failed, because the new password contains pattern from the previous password according to the sub_str_len defined in the password policy.
16 Password too long	The password change failed, because the new password is too long according to the maximum defined in the password policy.
20 Passwords do not match	The password change failed, because the new password does not match the password entered in the confirm password field.
21 Cannot include predefined prohibited characters	The password change failed, because the new password contains prohibited characters according to the password policy.
22 Password previously used	Privileged Access Manager denies access because the password that you entered was used before. Make sure that the new password you use conforms with the password policy rules.
23 Password is contained by a previous password or vice versa	The password change attempt failed because the password used is contained by a previous password or that the previous password is contained in the new password. You should select a new password that does not contain a previously used password.
24 Password is in dictionary file	The password change failed, because the new password is defined in the DICTIONARY class or DICTIONARY file. You should select a password that is not defined in the DICTIONARY class or in the DICTIONARY file.
100 Bad arguments	<p>The password change failed, because invalid data was sent to the authorization engine.</p> <p>Privileged Access Manager may write this message to the audit log when one of the following occurs:</p> <ul style="list-style-type: none"> <li>• A memory problem</li> <li>• A mismatch between versions of Privileged Access Manager various modules to a recent upgrade of the product</li> </ul> <p>Verify that there are no mixed Privileged Access Manager environments and that the client and server use the same version of the product. For assistance, contact CA Support at <a href="http://ca.com/support">http://ca.com/support</a>.</p>

## Authorization Stage Codes for Resource Access Events

Authorization stage codes for resource access events describe at which stage Privileged Access Manager decided to take action for the resource access event.

Authorization Stage Code	Indicates
50 Security LABEL check of resource	<p>Privileged Access Manager denied access to the resource, because <i>one</i> of the following is true for the user who tried to access the resource:</p> <ul style="list-style-type: none"> <li>• The resource security label has a higher security level than the user security label</li> <li>• The user does not have a security label</li> </ul>

51 Security LEVEL check of resource	Privileged Access Manager denied access to the resource, because <i>one</i> of the following is true for the user who tried to access the resource: <ul style="list-style-type: none"> <li>The resource has a higher security level than the user</li> <li>The user does not have a security level</li> </ul>
52 Category check of resource	Privileged Access Manager denied access to the resource, because the resource is assigned a security category that is not assigned to the user.
53 Resource DAYTIME check	Privileged Access Manager denied access to the resource, because the user attempted access at a time outside the permitted day and time for the resource.
54 OWNER check of resource	Privileged Access Manager permitted access to a resource, because the accessing user owns the resource.
55 Resource ACL check	Privileged Access Manager permitted or denied access to the resource, because the resource ACL lists the user.
56 In resource group ACL check	Privileged Access Manager permitted or denied access to the resource, because the resource group ACL lists list the user.
57 User group in resource ACL	Privileged Access Manager permitted or denied access to the resource because the user group ACL list at least one of the resource.
58 User group in resource group ACL	Privileged Access Manager permitted or denied access to the resource, because the resource group ACL lists at least one of the user group.
59 Resource UACC check	Privileged Access Manager permitted access to the resource, because of the resource's default settings.
61 User is OPERATOR on resource	Privileged Access Manager permitted access to the resource, because the user has the OPERATOR attribute. The OPERATOR attribute lets users bypass authorization procedures for read and chdir access for FILE resources. On UNIX, Privileged Access Manager writes this message to the trace file only, and does not write the message to the audit log file.
62 UACC check for Class of unprotected resource	Privileged Access Manager permitted or denied access to a resource that does not have a record in the product database, based on the defaccess value in the resource class.
63 Program Conditional Access	Privileged Access Manager permitted or denied access to the resource, because the resource PACL lists the program and the user or one of the user's groups.
64 User '*' in resource ACL	Privileged Access Manager permitted or denied access to the resource, because the resource ACL contains an asterisk (*). An asterisk specifies all defined users.
65 User is AUDITOR on resource	Privileged Access Manager permitted access to the audit file, because the user has the AUDITOR attribute. The AUDITOR attribute lets users bypass authorization procedures for read and chdir access requests. Privileged Access Manager writes this message to the trace file only, and does not write the message to the audit log file.
69 No step that allowed access	Privileged Access Manager denied access to the resource because it could not find a rule that let the user access the resource.



70 OWNER check of resource's group	Privileged Access Manager permitted access to the resource because the user attempting to access the resource is the owner of one of the resource's groups.
75 User '*' in resource group ACL	Privileged Access Manager permitted or denied access to the resource because the resource group ACL contains an asterisk (*). An asterisk specifies all defined users.
76 Resource denied ACL check	Privileged Access Manager denied access to the resource, because the resource NACL lists the user.
77 In resource group denied ACL check	Privileged Access Manager denied access to the resource, because the resource group NACL lists the user.
78 User group in resource denied ACL	Privileged Access Manager denied access to the resource, because the resource NACL lists at least one of the user groups.
79 User group in resource group denied ACL	Privileged Access Manager denied access to the resource, because the resource group NACL lists at least one of the user groups.
80 User '*' in resource denied ACL	Privileged Access Manager denied access to the resource, because the resource NACL contains an asterisk (*). An asterisk specifies all defined users.
81 User '*' in resource group denied ACL	Privileged Access Manager denied access to the resource, because the resource group NACL contains an asterisk (*). An asterisk specifies all defined users.
82 Group of resource DAYTIME check	Privileged Access Manager denied access to the resource, because the user attempted to access the resource at a time outside the permitted day and time for the resource group.
86 Resource calendar ACL check for user	Privileged Access Manager permitted or denied access to the resource, because the user attempted to access the resource at a time permitted or denied by the resource CALACL.
87 Resource group calendar ACL check for user	Privileged Access Manager permitted or denied access to the resource, because the user attempted to access the resource at a time permitted or denied by the resource group CALACL.
88 Resource calendar ACL check for user groups	Privileged Access Manager permitted or denied access to the resource, because the user attempted to access the resource at a time permitted or denied because the user is a member of one of the groups that are listed in the resource CALACL.
89 Resource group calendar ACL check for user groups	Privileged Access Manager permitted or denied access to the resource, because the user group attempted to access the resource at a time permitted or denied because the user is a member in one of the group's that are listed in the resource CALACL.
90 User * in resource calendar ACL	Privileged Access Manager permitted or denied access to the resource, because the resource CALACL contains an asterisk (*). An asterisk specifies all defined users.
91 User * in resource groups calendar ACL	Privileged Access Manager permitted or denied access to the resource, because the resource group CALACL contains an asterisk (*). An asterisk specifies all defined users.
92 Attempt to rename the path of a protected resource	<b>Valid on Windows</b> Privileged Access Manager denied a request to rename a protected file or registry entry.



200 Class checks not active	Privileged Access Manager permitted access to a resource, because the resource class is inactive. When a resource class is inactive, the setoptions list command displays the class activity as 'No'.
201 Loading the user information	Privileged Access Manager could not authorize a request, because it failed to retrieve a user's information.
202 Resource in WARNING mode	Privileged Access Manager permitted access to a resource, because the resource is in Warning Mode.
203 Access for the resource is MAXIMUM_ALLOWED	<b>Valid on Windows</b> When permitted, indicates that Privileged Access Manager assigned maximum access rights to the registry handle. When denied, indicates that Privileged Access Manager blocked access to the registry handle.
204 Class in WARNING mode	Privileged Access Manager permitted access to a resource, because the resource class is in Warning Mode.
210 Special kernel module load check	<b>Valid on UNIX</b> Privileged Access Manager permitted or denied the loading or unloading of the kernel module, based on the KMODULE class definitions.
250 Executing an untrusted program	Privileged Access Manager denied an attempt to execute an untrusted program.
251 Using deniable parameter	Privileged Access Manager denied an attempt to execute sesudo command, because the command syntax contains parameters the SUDO record defines as prohibited.
252 Relative path specified by an _abspath user	<b>Valid on UNIX</b> Privileged Access Manager denied an attempt to execute a program that was specified by a relative path, because the user attempting to execute the program is a member of the '_abspath' group.
253 Permitted sesudo job	Privileged Access Manager permitted an attempt to execute a sesudo command.
254 sesudo command failed	<b>Valid on UNIX</b> A sesudo command failed to execute on the operating system.
440 Invalid calendar was detected	Privileged Access Manager denied access because of an error in getting the calendar information. Example: a memory problem or calendar table corruption.
441 Calendar does not allow access	Privileged Access Manager denied access because the calendar object's definitions associated with the accessed resource do not allow access at this time.
1050 Default Record Security Label Check	Privileged Access Manager denied access to the default record, because <i>one</i> of the following is true for the user who tried to access the resource: <ul style="list-style-type: none"> <li>The resource security label has a higher security level than the user security label</li> <li>The user does not have a security label</li> </ul>
1051 Default Record Security Level Check	Privileged Access Manager denied access to the default resource, because <i>one</i> of the following is true for the user who tried to access the resource: <ul style="list-style-type: none"> <li>The resource has a higher security level than the user</li> <li>The user does not have a security level</li> </ul>

1052 Default Record Category Check	Privileged Access Manager denied access to the default resource, because the resource is assigned a security category that is not assigned to the user.
1053 Default Record Day and Time Check	Privileged Access Manager denied access to the default resource, because the user attempted access at a time outside the permitted day and time for the resource.
1054 Default Record OWNER Check	Privileged Access Manager permitted access to the default resource, because the accessing user owns the default resource.
1055 Default Record ACL Check for User	Privileged Access Manager permitted or denied access to the default resource, because the resource ACL lists or does not list the user
1056 Default Record Group ACL Check For User	Privileged Access Manager permitted or denied access to the default resource, because the resource group ACL lists or does not list the user.
1057 Default Record ACL Check for User Groups	Privileged Access Manager permitted read or chdir access to the default resource. Privileged Access Manager writes this message to the trace file only, and does not write the message to the audit log file.
1058 Default Record Group ACL Check for User Groups	Privileged Access Manager permitted or denied access to the default resource, because the resource group ACL lists or does not list the user group.
1059 Default Record Universal Access Check	Privileged Access Manager permitted access to the default resource, because of the resource's default settings.
1061 Default Record OPERATOR Attribute Check	Privileged Access Manager permitted access to the default resource, because the user has the OPERATOR attribute. The OPERATOR attribute lets users bypass authorization procedures for read and chdir access requests. Privileged Access Manager writes this message to the trace file only, and does not write the message to the audit log file.
1062 Default Record Class Global Universal Access	Privileged Access Manager permitted or denied access to the default resource that does not have a record in the product database, based on the defaccess value in the resource class.
1063 Default Record Program Conditional Access	Privileged Access Manager permitted or denied access to the default resource, because the resource PACL lists or does not list the program accessing the resource.
1064 User '*' in _default record ACL	Privileged Access Manager permitted or denied access to the default resource, because the resource ACL contains an asterisk (*). An asterisk specifies all defined users.
1069 No Rule Granting Access to Default Record	Privileged Access Manager denied access to the default resource because it could not find a rule that let the user access the resource.
1202 Default Record in WARNING Mode	Privileged Access Manager permitted access to the default resource, because the resource is in Warning Mode.
1250 Default Record is Set Untrusted	Privileged Access Manager denied an attempt to execute the default untrusted program.

## Authorization Stage Codes for Security Database Administration Events

Authorization stage codes for security database administration events describe at which stage Privileged Access Manager decided what action to take for the security database administration event.

Authorization Stage Code	Indicates
300 Undefined Privileged Access Manager user	Privileged Access Manager denied access to the system, because the accessing user could not be found in the product database. Check the user account profile.
301 An attempt to delete last ADMIN user	Privileged Access Manager denied a request to do one of the following: <ul style="list-style-type: none"> <li>Delete the last ADMIN user from the product database</li> <li>Remove the ADMIN attribute from the only user that is assigned the ADMIN attribute</li> </ul>
302 An attempt to delete user root	<b>Valid on UNIX</b> Privileged Access Manager denied an attempt to delete the system root account.
303 User trying to change their own password	Privileged Access Manager denied a user attempt to use a <code>selang</code> command to change their own password. On UNIX, change your password using the <code>sepass</code> utility. On Windows, change your password using native password management tools.
304 Nonauditor user trying to set audit mode	Privileged Access Manager denied a user attempt to change the audit mode of a record, because the user does not have the AUDITOR attribute. To let the user change the audit mode of a record, assign the user the AUDITOR attribute.
305 Command allowed for ADMIN user	Privileged Access Manager permitted an action, because the user requesting the action has the ADMIN attribute.
306 Showuser (myself) , Showxusr allowed	Privileged Access Manager permitted a user or an external user to display the properties of their own record in the product database. This message is not written as an audit record.
307 User trying to set categories they do not have	Privileged Access Manager denied an attempt to assign a security category to a user, because the user attempting to assign the security category does not possess that security category themselves.
308 User trying to set a security-label they do not have	Privileged Access Manager denied an attempt to assign a security label to a user, because the user attempting to assign the security label does not possess that security label themselves.
309 User trying to set security-level greater than the user's own	Privileged Access Manager denied an attempt to assign a security level to a user, because the user has a lower security level than the security level they are attempting to assign.
310 NonADMIN user trying to set user-mode	Privileged Access Manager denied an attempt to set an administrative attribute, because the user attempting to set the attribute does not have the ADMIN attribute.
311 Command allowed for object owner	Privileged Access Manager permitted an action, because the user owns the record.
312 Native file owner can define it to Privileged Access Manager	<b>Valid on UNIX</b> Privileged Access Manager permitted an action, because the file owner defined the file to the product.  <b>Note:</b> A file owner can define a file to Privileged Access Manager when the <code>use_unix_file_owner</code> token in the <code>lang</code> section of the <code>seos.ini</code> file is set to yes.

313 Command allowed for a GROUP-ADMIN user	Privileged Access Manager permitted a user with the GROUP-ADMIN attribute to modify a record within the group.
314 GROUP-ADMIN user can join join- to group	Privileged Access Manager permitted a user with the GROUP-ADMIN attribute add or remove a user to the group.
315 GROUP-AUDITOR ADMIN can list the group	Privileged Access Manager permitted a user to list the properties of a record within a group, because the user has the GROUP-ADMIN or GROUP-AUDITOR attribute for that group.
316 An auditor can list any object	Privileged Access Manager permitted a user with the AUDITOR attribute to display data in the database.
317 An OPERATOR can list any object	Privileged Access Manager permitted a user with the OPERATOR attribute to display data in the database
318 A GROUP-AUDITOR can list objects in group scope	Privileged Access Manager permitted a user with the GROUP-AUDITOR attribute to display data about the group in the database.
319 A GROUP-OPERATOR can list objects in group scope	Privileged Access Manager permitted a user with the GROUP-OPERATOR attribute to display data about the group in the database.
320 Command allowed for CLASS-ADMIN user	Privileged Access Manager permitted the action, because the action was performed by a user listed in the ACL of the ADMIN class.
321 Command allowed for PWMANAGER ADMIN with access	Privileged Access Manager permitted a user to change a password, because the user has the PWMANAGER or ADMIN attribute.
322 There is no rule allowing this operation	Privileged Access Manager denied an operation, because no rule that permitted the operation was found.
324 User changing their own password using sepass	Privileged Access Manager permitted a user to use the sepass utility or the password policy model to change their password.
326 User created 'Login Information' for themselves	Privileged Access Manager permitted a user to created login information for themselves.
327 Command allowed for GROUP-PWMANAGER	Privileged Access Manager permitted the command, because the user that executed the command has the GROUP-PWMANAGER attribute.
329 A PWMANAGER enabled a user	Privileged Access Manager permitted a user to enable (re-activate) another user, because the user that enabled the other user has the PWMANAGER attribute.
330 Command allowed for DOMAIN change	<b>Valid on Windows</b> Privileged Access Manager permitted the user to change the DOMAIN class, for example, adding new computers to the domain
331 Command allowed for PWMANAGER	Privileged Access Manager permitted the command to execute, because the user that executed the command has the PWMANAGER attribute.
332 Changing native flags allowed for PWMANAGER	<b>Valid on Windows</b> Privileged Access Manager permitted the user to modify the account flags assigned to a user account, because the user has the PWMANAGER attribute.
333 Changing 'must change password next logon' attribute is allowed for PWMANAGER	<b>Valid for Windows</b> Privileged Access Manager permitted the user to modify the 'must change password next logon' attribute for a user account, because the user has the PWMANAGER attribute.

334 Command allowed for GROUP-PWMANAGER	Privileged Access Manager permitted the command, because the user that executed the command has the GROUP-PWMANAGER attribute
335 Editing 'Login Information' is allowed for PWMANAGER	Privileged Access Manager permitted the user to edit the 'Login Information' attribute for a user account, because the user has the PWMANAGER attribute.
336 Command allowed for auditor user	Privileged Access Manager permitted a user to execute a command, because the user has the AUDITOR attribute.
337 Failed to reconcile command with database information	Privileged Access Manager did not execute a command, because the objects embedded in the command do not exist in the product database. Check the command syntax before you re-execute the command.
338 Creating a command from an implicit request	Privileged Access Manager created a command that originated from an implicit request.
339 SEOS_syscall module unload readiness check	<b>Valid on UNIX</b> An accessor is executing the 'secons scl' command to check if there are processes running in the intercepted syscalls. The product does not permit unloading the SEOS_syscall module.
340 Command allowed for ADMIN group	<b>Valid on UNIX</b> Privileged Access Manager permitted an action, because the user has the ADMIN attribute.
341 Command allowed for AUDITOR group	<b>Valid on UNIX</b> Privileged Access Manager permitted an action, because the user has the AUDITOR attribute.
342 Command allowed for OPERATOR group	Privileged Access Manager permitted an action, because the user has the OPERATOR attribute.
343 Command allowed for PWMANAGER group	<b>Valid on UNIX</b> Privileged Access Manager permitted an action, because the user has the PWMANAGER attribute.
344 Command allowed for SERVER group	<b>Valid on UNIX</b> Privileged Access Manager permitted an action, because the user has the SERVER attribute.

## Authorization Stage Codes for Shutdown Events

Authorization stage codes for shutdown events describe at which stage Privileged Access Manager decided what action to take for the shutdown event.

Authorization Stage Code	Indicates
451 User is an OPERATOR	Privileged Access Manager permitted the shutdown request, because the user that executed the shutdown sequence has the OPERATOR attribute.
452 User is ADMIN or SPECIAL	Privileged Access Manager permitted the shutdown request, because the user executing the shutdown sequence has the ADMIN attribute assigned to him.

453 _seagent is allowed to shutdown Privileged Access Manager	<b>Valid on UNIX</b> Privileged Access Manager permitted the shutdown request, because _seagent is permitted to shut down the product.
455 Daemon shut down by root (UNIX)	<b>Valid on UNIX</b> The seosd Daemon was shut down by root after the watchdog requested a restart.
456 Daemon shut down by watchdog	<b>Valid on Windows</b> The watchdog has requested a Privileged Access Manager license so it can restart the engine.
460 User is not allowed to shutdown Privileged Access Manager	Privileged Access Manager denied the shutdown request, because the requesting user is not permitted to shut down the product.
600 Attempting to Terminate Privileged Access Manager	Privileged Access Manager denied the shutdown request, because the user attempted to terminate the product by executing the kill command.

## Authorization Stage Codes for Trace Message On a User

Authorization stage codes for trace events on a user describe at which stage Privileged Access Manager decided what action to take for the user activity event.

Authorization Stage Code	Indicates
994 Informational Message	A user accessed the trace audit records. This is an informative message only, viewed by running the seaudit tr command.
995 Unauthorized Access to Internal Resource	An accessor attempted an unauthorized access to an internally protected FILE resource. Example: seos.audit records.
996 Authorized Access to Internal Resource	Privileged Access Manager permitted access to the resource by an internal bypass. Example: reading /etc/passwd.
997 User Can Execute a setuid setgid Directory	<b>UNIX only</b> Privileged Access Manager bypassed an event because an accessor attempted to execute a directory marked with a setuid \setgid flag bit. This stage is part of a TRACE record message.
998 Authorization is Configured as 'Audit Mode Only'	<b>Windows only</b> Privileged Access Manager is set to work in 'Audit Mode Only'.
999 Resource not Protected (Check if Rules Exists)	Privileged Access Manager permits access to an unprotected resource.

## Authorization Stage Codes for Untrust Message Events

Authorization stage codes for untrust message events describe at which stage Privileged Access Manager decided on what action to take for the untrust message event.

Authorization Stage Code	Indicates
0 A general error occurred during Watchdog file checking	An error occurred while Privileged Access Manager fetched the file information. The product can write this message to the audit log if the file is untrusted. Check the system logs for more information.
1 Stat information of PROGRAM or SECFILE was changed	Data changed in a record in the PROGRAM or SECFILE classes. Privileged Access Manager can write this message to the audit log if it detects an attempt to tamper with a program or file. Check the audit events, system logs, and trace records for the program or file. If an administrator changed the program or file, consider re-trusting the changed program or file.
4 CRC check of PROGRAM or SECFILE changed	The Cyclic Redundancy Check (CRC) changed of a record in the PROGRAM or SECFILE class. Check the system logs, event log files, and trace records for the program or file.
5 Cannot stat file of PROGRAM or SECFILE	Privileged Access Manager failed to retrieve file information for the specified file. The product can write this message to the audit log if one of the following events occurs: <ul style="list-style-type: none"> <li>• The file name or directory changed</li> <li>• The file name or directory does not exist</li> <li>• The access permissions of the file</li> <li>• The system is out of memory</li> </ul> To determine the possible cause of the error, check the system log files.
7 MD5 signature of PROGRAM or SECFILE changed	The MD5 signature changed for a record in the PROGRAM or SECFILE classes. Check the system log files, audit messages, and trace logs for the program or file.
8 SHA1 signature of PROGRAM or SECFILE changed	The SHA1 signature changed for a record in the PROGRAM or SECFILE classes. Check the system log files, audit messages, and trace logs for the program or file.
10 SHA256 signature of PROGRAM or SECFILE changes	The SHA256 signature changed for a record in the PROGRAM or SECFILE classes. Check the system log files, audit messages, and trace logs for the program or file.
11 SHA384 signature of PROGRAM or SECFILE changed	The SHA384 signature changed for a record in the PROGRAM or SECFILE classes. Check the system log files, audit messages, and trace logs for the program or file.
12 SHA512 signature of PROGRAM or SECFILE changed	The SHA512 signature changed for a record in the PROGRAM or SECFILE classes. Check the system log files, audit messages, and trace logs for the program or file.

## Reason Codes That Specify Why a Record Was Created

Reason codes that specify why a record was created describe at which stage Privileged Access Manager decided what audit record to create for the event.

Reason Code	Why Privileged Access Manager Logged this Operation
0 No specific request to log the operation	No specific request to log in the operation exists so it was logged by default.
2 User audit mode requires logging	The audit property of the accessor or its profile matches the record's result. Example: an action performed by a user with the FAILURE value set for the AUDIT_MODE property is logged only when the user fails to access a protected resource.
3 Resource audit mode required logging	The RAUDIT property of the resource matches the record's result.
4 Resource in WARNING mode	A WARNING property was set to the resource or to the resource's class.
5 Privileged Access Manager serevu utility requested auditing	<b>Valid on UNIX</b> The serevu utility requested the audit record. Example: when a user attempt to log in fails.
7 Outbound connection record	<b>Valid on UNIX</b> A successful outbound connection occurred.
8 Privileged Access Manager pam support UNIX failed login	<b>Valid on UNIX</b> The Privileged Access Manager PAM module requested the audit. Example: in an event of a failed password login attempt.
9 Daytime restrictions check of CALENDAR class	A daytime restrictions check of a CALENDAR class required logging an audit record.
10 A specific request to log operation	A specific request was made to log the operation. Example: attempting to kill the Privileged Access Manager daemons.
11 Privileged Access Manager secons utility requested auditing	<b>Valid on UNIX</b> The Syscall monitor option is sued (secons-scl).

## selang Reference Guide

This guide provides information about Privileged Access Manager selang command, database classes and properties, and Windows values. This guide is also provided with Privileged Access Manager, which offers enterprise management and reporting capabilities, and advanced policy management features.

### Command Line Interpreter

#### Contents

Privileged Access Manager is administered through a command shell that is known as selang, the Privileged Access Manager command language. The selang command language lets you make definitions in the Privileged Access Manager database. The selang command language is the command definition language.

The selang utility is located in the bin directory of your Privileged Access Manager installation. When you enter the selang shell, a special selang prompt appears. The exact form of the prompt depends on your working environment. The prompt looks similar to this:



PAMSC>

The selang command shell operates on the local database by default. To operate on the Privileged Access Manager database of a different station, specify the hosts command before entering the selang commands.

**selang Utility** Run the Privileged Access Manager Command Line

The selang utility invokes a command shell that provides access to the Privileged Access Manager database and the native environment. The database is updated dynamically by issuing selang commands from within the command shell.

#### NOTE

The result of the execution of the command is sent to the standard output unless you include the -o option.

This command has the following format on UNIX:

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] \
```

```
[-u userpass]
```

```
selang [-l] [-o file] [-r file] [-s] [-u userpass]
```

This command has the following format on Windows:

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] [-v]
```

```
selang [-l] [-o file] [-r file] [-s] [-v]
```

- **-c *command***

Specifies the selang command to execute. After selang executes the command, it exits.

If *command* contains any spaces, enclose the entire string in quotation marks. For example:

```
selang -c "showusr rosa"
```

- **-d *path***

Specifies that selang commands update the database in the defined path.

**Note:** You can only specify a local database.

- **-f *file***

Specifies that selang commands are read from the defined file rather than from the standard input of the terminal. As selang executes the commands in the input file, the line number of command being executed appears on the screen. The selang prompt does not appear on the screen. After selang executes the commands in *file*, it exits.

- **-h**

Displays the help for this utility.

- **-l**

Specifies that selang updates the default local database, usually *ACInstallDir/seosdb* (where *ACInstallDir* is the directory where you installed Privileged Access Manager).

You do not need to specify this option with -d or -p.

**NOTE**

This option replaces `selang`. It is only valid when `seosd` is not running, and only a Privileged Access Manager administrator with sufficient native privileges to update the database files can execute it.

- **-o *file***  
Specifies that `selang` output is written in the specified file. Each time that you invoke `selang`, it creates a new, empty file. If you specify the name of an existing file, `selang` writes over the information currently in the file.
- **-p *pmdb***  
Specifies that `selang` commands update the database of the defined PMDB, which must be in the local station (this is the database in the PMDB subdirectory). Changes to the database are not propagated to subscribers.

**NOTE**

This option is not valid if either `sepmdd` or `seosd` is running on the specified PMDB. This option is not the same as using the *hosts command*.

**WARNING**

Do not make changes that require propagation in this mode. If you use native mode when making updates, Privileged Access Manager updates only the native host files (as defined in the product configuration options).

- **-r *file***  
Specifies that `selang` reads the commands from the defined file. The file should consist of commands in normal `selang` syntax, which is separated by semicolons or line breaks. After you execute the commands in *file*, `selang` prompts the user for input.  
If you do not define a file for this option, `selang` uses the `.selangrc` file in your home directory.
- **-s**  
Specifies that `selang` opens in silent mode, without displaying the copyright message.
- **-u *user pass***  
(UNIX only) Specifies a username and password for running `selang`.  
To use this option, set the `check_password` token in the `seos.ini` file to `yes`. This token causes Privileged Access Manager to prompt you with Enter your password when you run `selang -u`. You have three attempts to log in. The token `no_check_password_users` in the `[lang]` section of the `seos.ini` file contains a list of users that bypass the password checking during a login to `selang`.

**NOTE**

If the `check_password` token is set to `no` (the default), `selang` does not require any passwords.

- **-v**  
(Windows only) Writes command line to output.

Usage notes:

- If `-h` is used, all other options are ignored.
- You cannot use the `-c` option with the `-f` option.
- You cannot use the `-d` option with the `-p` option.
- If you specify `-d` or `-p`, you do not need to specify `-l`.

## Features of the `selang` Command Shell

After you enter the `selang` command shell, the following prompt appears:

```
PAMSC>
```

When the prompt appears, you can enter `selang` commands. Enter commands that are separated with a semi-colon (;). To enter a command on more than one line, type a backslash (\) at the end of a line to continue typing the command on the

next line. You can edit the command line. Use the left and right arrow keys to move around within the line. You can insert characters by typing them directly in place, and delete characters with the standard Backspace and Delete keys, or on UNIX, by pressing Ctrl+D.

selang supports many of the command line entry features available in UNIX shell tcsh and other smart shells. These include the following features:

- Special characters
- Shortcut keys
- Command history
- Special features

#### NOTE

On UNIX, you can use a *UNIX exit* which is a program that you can specify-a shell script or an executable-to run automatically before or after a user or group is added or updated. For more information about UNIX exits, see the *Endpoint Administration Guide for UNIX*.

## Special Characters

selang supports the following special characters:

Character	Description	Meaning
# or *	Pound (hash) or asterisk	At the beginning of a line, indicates that the line is a comment; the line is not executed. Comment lines are useful when inputting the selang commands from a file.
!	Exclamation mark	At the beginning of the line, indicates that the rest of the line is a shell command. selang sends the command to the operating system shell program for execution; Privileged Access Manager does not execute the line.
\	Backslash	As the last character of a line, indicates the command continues on the following line.
;	Semicolon	Terminates a command and introduces a new command on the same line.
	Pipe	Sends the output of the preceding command to the input of the succeeding command (the specified <i>pipe</i> ).

## Shortcut Keys

selang supports the following shortcut keys:

Key	Valid on	Meaning
Up-arrow, Down-arrow, or ^	All	Used to navigate and retrieve a command from the command history.
Tab	UNIX	Serves for word completion.

Ctrl+D	UNIX	With the cursor positioned at the end of the line, displays a list of words that match the word completion string in the command line.  With the cursor positioned anywhere else on the line, deletes the character to the right of the cursor.
Esc, Esc Ctrl+2	UNIX	Displays the help text for the command in the command line. All the text in the command line is preserved, so that you can continue typing the command from where you left off.
F1	Windows	Inserts the previous command, character by character.
F2	Windows	Displays a window with the instruction: Enter char to copy up to: When you enter a character from the previous command, selang enters the command up to the first instance of the character. If the character occurs more than once in the command, you can press F2 again to insert up to the next instance.  Use Backspace to cancel.
F3	Windows	Enters the previous command (same as up arrow).
F4	Windows	Edits the previous instruction. Displays a window with the instruction: Enter char to delete up to:  Use Backspace to cancel.
F5	Windows	Enters the previous command (same as up arrow).
F6	Windows	Enters a Ctrl Z (^Z) in the command line. This allows you to press Enter and continue entering the command on the next line.
F7	Windows	Displays a window listing the command history. You can use the up and down arrows to select any previous command.  Use Esc to cancel.
F8	Windows	Enters the previous command, as the up arrow does, but with the cursor positioned at the beginning of the command line rather than at the end.
F9	Windows	Displays a window with the instruction: Enter command number: The number you enter inserts the command with the corresponding number in the F7 listing.  Use Esc to cancel.

## Command History

selang stores executed commands in a *history list*. Use the up and down arrow keys to display commands in the command line from the history list. To see only the commands that start with a specific character or string, type the

beginning of the command before using the up and down arrows. When you press *Enter*, the text currently displayed in the command line is executed.

To view previously issued commands, enter the history command.

The selang command shell supports the following shortcuts that use the commands stored in the history list:

Shortcut	Runs
<b>^^</b> [ <i>string</i> ]	The previous command. If you specify <i>string</i> , selang appends it to the original command.
<b>^n</b> [ <i>string</i> ]	The <i>n</i> th command in the history list, where <i>n</i> is a positive integer. If you specify <i>string</i> , selang appends it to the original command.
<b>^-n</b> [ <i>string</i> ]	The <i>n</i> th command from the end of the list, where <i>n</i> is a positive integer. If you specify <i>string</i> , selang appends it to the original command.
<b>^mask</b> [ <i>string</i> ]	The most recently issued command that begins with <i>mask</i> , where <i>mask</i> is a text string. If you specify <i>string</i> , selang appends it to the original command.

#### NOTE

On Windows, you can use the F7 key to view the history list.

## Special Features

You can use several additional techniques to save keystrokes in the selang command shell.

#### NOTE

Record and class names are case-sensitive on UNIX but not on Windows.

- **Command Recognition**  
selang recognizes which command you want to execute as soon as you have typed in enough characters to distinguish it from all the other available commands. For example, you can type **ho** to run the *hosts* command as it is the only command beginning with those letters. As soon as you type **ho**, selang can recognize the intended command. On the other hand, there are several commands that begin with the string **new**. You must add enough characters to distinguish between *newusr*, *newgrp*, *newfile*, and *newres*.
- **Abbreviations**  
Each command is also associated with a one- to four-letter abbreviation. For example, because there are several commands beginning with the string *new*, you can also use the abbreviation **nu** for the command *newusr*. These abbreviations are documented as part of the command syntax for each command. You can enter commands in either uppercase or lowercase.
- **Word Completion (UNIX only)**  
Press *Tab* in the middle of a word to complete the word. Word completion is context-sensitive. If more than one word matches the specified string, selang uses the shortest word or word fragment that matches the string. For example, if you type the letter *n*, selang supplies *ew*, to form the word *new*. If this is not the required word, type another one or two characters and press *Tab* again to complete the word. Press **Ctrl+D** to see all the possible options. This is useful if you are not sure which command to use. Using the example in the previous paragraph, if you add the letter *u* to the word *new* and press *Tab*, selang supplies *sr*, giving you the command *newusr*. Words that are not part of the selang commands are stored in memory for use by the word completion feature later on in the same session. For example, if you type *newusr Mercedes*, and then later type *showusr Me* followed by *Tab*, the abbreviation *Me* is expanded to *Mercedes*, as follows:

```
showusr Mercedes
```

This assumes that you have not entered any other user name that begins with "Me".

## Wildcard Matching

selang supports the following wildcard characters:

- **\* (asterisk)**  
Any sequence of zero or more characters.
- **? (question mark)**  
Any single character (except a path separator for files).

To make a single character a do not care character that matches any other single character, use a question mark (?), as in the following examples:

Specify this...	To do this...
mmc?	mmc3, mmc4, mmc5
mmc?.t	mmc1.t, mmc2.t
mmc04.?	mmc04.a, mmc04.1

To match any string of zero or more characters, use an asterisk (\*), as in the following examples:

Specify this...	To do this...
*i*.c	main.c, list.c
st*.h	stdio.h, stdlib.h, string.h
*	All records of the specified class

## selang Command Authorization

To use selang commands that change records in the AC or native operating system (native OS) environment, you must have sufficient authority. For most commands, *one* of the following conditions must be met:

- You are the owner of the resource.
- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You have CREATE or MODIFY access authority in the ACL of the record in the ADMIN class.
- (Windows) If your installation only permits management of the native Windows environment, you are a member of the Privileged Access Manager Administrators group in the Windows database.
- (UNIX) If your installation only permits management of the native UNIX environment, you are a member of the Privileged Access Manager Administrators group in the security files of the local UNIX host.

### NOTE

Exceptions to these general rules are noted in the description of each command.

## Access Control List Support

To give or deny access authority, you can use six types of access control lists:

- **ACL**  
Standard access control list that contains the user names and group names authorized to access the resource and the level of access granted to each.
- **NACL**

Negative access control list that contains the user names or group names that are not authorized to access the resource.

- **PACL**

Program access control list that depends upon the accessing program. Each PACL contains the user names and group names, the level of access, and the name of the program or shell script the user must execute to access the particular resource.

- **INET-ACL**

Internet access control list.

- **CACL**

Conditional access control list.

- **AZNACL**

The authorization ACL; an ACL that allows access to a resource based on the resource description.

Privileged Access Manager uses all relevant lists when it checks a user's authority to access a resource.

#### NOTE

You can maintain any single list with a single authorize command. To change more than one list you need to issue authorize again. You cannot define multiple access rights for multiple users and groups with one authorization rule. You must separate the rules.

The following table lists which access control lists you can use with each class. Classes that do not appear in the table have no access control lists and cannot be controlled by the authorize command.

Class	ACL/ NACL	CALACL	PACL	INET-ACL	CACL	AZNACL
ADMIN	X	X	X			
APPL	X	X				X
AUTHHOST	X	X				X
CONNECT	X	X	X			
CONTAINER	X	X	X			
DOMAIN	X	X	X			
FILE	X	X	X			
GAPPL	X	X				X
GAUTHHOST	X	X				X
GFILE	X	X	X			
GHOST				X		
GSUDO	X	X				
GTERMINAL	X	X				
HOLIDAY	X	X				
HOST				X		
HOSTNET				X		
HOSTNP				X		
LOGINAPPL	X	X				
MFTERMINAL	X	X	X			
PROCESS	X	X	X			
PROGRAM	X	X				
REGKEY	X	X	X			
REGVAL	X	X	X			

SUDO	X	X	X			
SURROGATE	X	X	X			
TCP	X	X	X		X	
TERMINAL	X	X	X			
UACC	X	X				
USER_DIR	X					X

## Access Authority by Class

Valid access values depend on the class the resource belongs to. The following table lists valid access values by class in the AC environment.

Class	Valid Access Values	Lets Accessors...
All classes	all	Perform <i>all</i> valid operations for the class.
	none	Perform <i>no</i> valid operations for the class.
ADMIN	create	Create records in this class.
	delete	Delete records in this class.
	join	Add a group to a USER record and to complete the linking of a user to a group. <b>Note:</b> The accessor must also have <i>modify</i> access.
	modify	Modify existing records. <b>Note:</b> To link a user to a group (add user names to GROUP records) the accessor must also have <i>join</i> access.
	password	Change the passwords of other users. <b>Note:</b> This access type affects only the USER class.
	read	List records in this classes
AUTHHOST	read	Login from an authenticated host.
CONNECT	read	Connect to the remote host.
CONTAINER	<i>inherited</i>	<b>Note:</b> Valid access values for this class are the valid values for the class of the contained objects.
DOMAIN	chmod	Create and delete trust relationships between one domain and another. <b>Note:</b> Both domains must have this access type.
	execute	Add or delete members from the domain.
	read	List domain members.
FILE, GFILE	chdir	Access the directory with the equivalent of read and execute permissions.
	chmod	Change file system modes. <b>Note:</b> Only applicable on UNIX hosts.
	chown	Change the owner of the record.



	control	Perform <i>all</i> valid operations except <i>delete</i> and <i>rename</i> .
	create	Create records in this class.
	delete	Delete records in this class.
	execute	Execute a program. <b>Note:</b> The accessor must also have <i>read</i> access.
	read	Use a file or directory without changing it. <b>Note:</b> On UNIX, if you want <i>read</i> privileges to control whether users can perform operations that obtain information about the file (such as <i>ls -l</i> ), set the <i>STAT_intercept</i> configuration setting to 1. For more information, see the <i>Reference Guide</i> .
	rename	Rename to a record in this class.
	sec	Change the ACL of records in this class.
	update	Perform the combined operations of <i>read</i> , <i>write</i> , and <i>execute</i> .
	utime	Change the modification time of a file. <b>Note:</b> Only applicable on UNIX hosts.
	write	Change the file or directory.
HNODE	read	List records in the class.
	write	Edit the details of the record.
HOLIDAY	read	Log in during the specified holiday.
KMODULE	load	Load a kernel module.
	unload	Unload a kernel module.
MFTERMINAL	read	Log in from the Mainframe terminal.
	write	Administer from the Mainframe terminal.
POLICY	delete	Delete the policy.
	execute	Deploy the policy.
	read	View policy details.
	write	Edit the details of the record.
	undeploy	Perform the combined operations of <i>delete</i> and <i>execute</i> .
PROCESS	read	Kill the process.
PROGRAM, SUDO, GSUDO	execute	Execute a program.
REGKEY	delete	Delete a Windows registry key.
	read	List the contents of the Windows registry key.
	write	Change the Windows registry key.
REGVAL	delete	Delete a Windows registry value.
	read	Read a Windows registry value.
	write	Change a Windows registry value.
RULESET	read	View the details of the record.
	write	Edit the details of the record.

SURROGATE	execute	Surrogate to the user.
TCP	read	Access TCP services from remote hosts or host groups.
TERMINAL, GTERMINAL	read	Log in to the terminal.
	write	Administer the terminal.
UACC	<i>inherited</i>	<b>Note:</b> Valid access values for this class are the valid values for the class it is defining.
WINSERVICE	read	View the properties of the Windows service.
	start	Start the Windows service.
	modify	Change the properties of the Windows service.
	resume	Resume a paused Windows service.
	stop	Stop a Windows service.
	pause	Pause a Windows service.

**NOTE**

The values none and all are applicable to all classes. The value all represents the entire group of access values, other than none, for a particular class. For more information about access authority, see the *Endpoint Administration Guide* for your OS.

**Windows Access Authority by Class**

Valid access values depend on the class the resource belongs to. The following table lists valid access values by class in the Windows (nt) environment.

Class	Valid Access Values	Let Accessors...
All classes	all	Perform <i>all</i> valid operations for the class.
	none	Perform <i>no</i> valid operations for the class.
COM, DISK	change	Perform the combined operations of <i>delete</i> , <i>read</i> , and <i>write</i> .
	changepermissions	Modify the ACL of the resource.
	delete	Delete the resource.
	read	Access data on the resource without changing it.
	takeownership, chown, owner	Change the owner of the specified resource.
	write	Write data to the specified resource.
FILE		<b>Note:</b> It is only possible to define access authorities for NTFS files; FAT files cannot have access authorities.
	change	Perform the combined operations of <i>delete</i> , <i>read</i> , and <i>write</i> .
	changepermissions, sec	Modify the ACL of the resource.
	chmod	Perform all operations except <i>delete</i> .
	chown	Change the owner of the specified resource.

	delete	Delete the resource.
	execute	Execute programs. <b>Note:</b> To use this access, the accessor must also have <i>read</i> access.
	read	Access a resource without changing it.
	rename	Renames the resource. <b>Note:</b> To rename a file, you must have <i>delete</i> access to the source and <i>rename</i> access to the target. The audit log reflects this order of events.
	write	Modify the resource.
	update	Perform the combined operations of <i>read</i> , <i>write</i> , and <i>execute</i> .
PRINTER	manage	Manage the printer. For example, set the data for a specified printer, pause printing, resume printing, clear all print jobs, update the ACL, or change printer properties.
	print	Print using the printer.
REGKEY	append, create, subkey	Create or modify a subkey of the registry key
	takeownership, chown, owner	Change the owner of the resource
	changepermissions, sec, dac, writedac	Modify the ACL of the resource.
	delete	Delete the resource.
	enum	Enumerate subkeys.
	link	Create a link to the registry key.
	notify	Change notifications for a registry key or for subkeys of a registry key.
	query	Query a value of the registry key
	read	Access a resource without changing it.
	readcontrol, manage	Read the information in the registry key's security descriptor, not including the information in the system (audit) ACL.
	set	Create or set a value of the registry key.
	write	Change the registry key and its subkeys.
SHARE	change	Change properties of the resource or remove sharing from the resource.
	read	Access a resource without changing it.

**NOTE**

The values *none* and *all* are applicable to all classes. The value *all* represents the entire group of access values, other than *none*, for a particular class. For more information about access authority, see the *Endpoint Administration Guide for Windows*.

## selang Environments

In addition to working on the local Privileged Access Manager database, you can use selang to modify the following:

- The native (Windows or UNIX) database
- The local Policy Model database (PMDB)
- A database on a remote host (Windows or UNIX) where Privileged Access Manager is installed
- Privileged Access Manager configuration settings

To switch environments, use the *env* (environment) command, which is available in all environments.

Some commands are the same in the different environments, but they may have different parameters and arguments. You should, therefore, check the syntax carefully when beginning to work in a new environment.

#### NOTE

When you are entering the *native* property of a command using *env*, the command is entered in both the *native* environment and current environment.

The following environments are supported:

Environment	Command	Prompt	Description
Policy Model	<code>env pmd</code>	<code>PAMSC (pmd) &gt;</code>	All <i>selang</i> commands operate on the local PMDB.
Native Windows	<code>env nt</code>	<code>PAMSC (nt) &gt;</code>	All <i>selang</i> commands modify the Windows database.
AC	<code>env ac</code>	<code>PAMSC&gt;</code>	All <i>selang</i> commands operate on the Privileged Access Manager database.  <b>Note:</b> This is the default.
Native UNIX	<code>env unix</code>	<code>PAMSC (unix) &gt;</code>	All <i>selang</i> commands operate on the security files of the local UNIX host.
Native	<code>env native</code>	<code>PAMSC (native) &gt;</code>	All <i>selang</i> commands operate in the native environment of the host.
Remote Configuration	<code>env config</code>	<code>PAMSC (config) &gt;</code>	All <i>selang</i> commands operate on the Privileged Access Manager configuration settings for the host.

## selang Configuration on UNIX

On UNIX, you can manage the way *selang* works. Most of the options are concerned with the way *selang* manages the UNIX security system (for the *selang* UNIX environment).

The *selang* utility uses the following two files for configuration options:

- **seos.ini**  
Contains the product configuration options. This is the main configuration file for the product.
- **lang.ini**  
Contains configuration information that *selang* uses.

*selang* uses the *lang.ini* files in *one or both* of the following locations:

- The directory where the seos.ini file is located.
- Home directory of the user.

If you specify a token in only one of these lang.ini files, selang uses the value from that file. If you specify a token differently in the two lang.ini files, the value in the home directory of user overrides the other one.

The values for the tokens DefaultShell and DefaultHome in the seos.ini file of server *override* the values set in the tokens DefaultShell and HomeDirPrefix in the lang.ini file.

**Note:** Sample lang.ini files are located in the directory *ACInstallDir/samples/lang.init*.

## Change the User File

The default file for updating UNIX users is /etc/passwd but you can change this default. This is normally required on the NIS server if you are working under NIS.

To change the user file modify the *YpServerPasswd* in the *passwd* section of the seos.ini file to point to your user's file full pathname.

## Change the File for Updating Groups

The default file for updating UNIX groups is /etc/group but you can change this default. This is normally required on the NIS server if you are working under NIS.

To change the file for updating groups modify the **YpServerGroup** in the **passwd** section of the **seos.ini** file to point to your user's file full pathname.

## Automatic Backup of the UNIX User and Group Files

Before the first update of a UNIX user in a session and before the first update of a UNIX group in a session, Privileged Access Manager creates a backup copy of the files /etc/passwd or /etc/group. The backup files are called /etc/passwd.SeOS.bak and /etc/group.SeOS.bak, respectively. If an error occurs when updating the UNIX system, the original information is recoverable. Backups are made only before the first change to the UNIX system in a selang command shell session.

## Get selang Help

You can get help at any time in the interactive selang command environment.

To enter selang online help, enter one of the following:

- **? or help**  
The selang online help text for the environment you are in, appears on the screen, displaying the table of contents.
- **help topic**
  - *topic*  
Defines a selang command or other topic related to the selang command shell.  
The help text that describes the topic appears.
- **help env**
  - *env*  
Defines is a selang environment.  
The help text for the specified environment appears on the screen, displaying the table of contents.

**NOTE**

On UNIX, to display the help text for a command typed in the command line without deleting the text in the command line, type Ctrl+2 (or press Esc, Esc).

## Rules Effectiveness Exceptions

Most rules created by selang command become effective shortly after creation with the following exceptions:

- **SPECIALPGM class**  
Newly created or changed SPECIALPGM rules become effective for newly executed programs or after you restart Privileged Access Manager.
- **USER Class**  
Audit, trace, and interactive attributes become effective for new login sessions.

## selang Commands Reference

The following table lists all selang commands alphabetically.

**NOTE**

Commands that operate in the same manner in all environments are documented only in the AC environment. However, some commands are valid in more than one environment but differ in the manner they operate in each environment. These commands are marked with an asterisk (\*) in the *Description* column of the table below and are documented separately in each environment they are valid in.

Command	Short	Environments	Description
alias		AC and unix <b>Note:</b> For UNIX hosts only.	Lists or defines aliases for selang commands and properties.
authorize	auth	AC and nt	*Sets the authority a specific accessor has when accessing a specific resource.
authorize-	auth-	AC and nt	*Removes the authority previously given to a specific accessor when accessing a specific resource.
backuppmd		pmd	Backs up the data in the PMDB database to a specified directory.
check		AC	Checks whether a user has access privileges to a particular resource.
checklogin		AC	Determines a user's login privileges, whether a password check is needed, and whether a terminal access check is needed.
checkpwd		AC	Checks a user's new password, without changing it, to make sure it follows password rules.
chfile	cf	AC and native	*Changes the definition of a file record in the Privileged Access Manager or native OS database.

chgrp	cg	AC and native	*Changes existing internal group settings in the Privileged Access Manager or native OS database.
chres	cr	AC and nt	*Changes an existing resource record in the Privileged Access Manager or native OS database.
chusr	cu	AC and native	*Changes an existing internal user in the Privileged Access Manager or native OS database.
chxgrp	cxg	AC	Changes existing enterprise group settings in the Privileged Access Manager database.
chxusr	cxu	AC	Changes existing enterprise user settings in the Privileged Access Manager database.
createpmd		pmd	Creates a PMDB on a remote host.
deletepmd		pmd	Removes the PMDB's selang protection files, the contents of the PMDB directory, and the PMDB directory from the remote host.
deploy	◆ ◆	AC	Executes deployment selang commands stored in a RULESET object for the particular POLICY.
deploy-		AC	Executes policy undeployment selang commands stored in a RULESET object for the particular POLICY.
editfile	ef	AC and native	*Adds or changes the definition of a file record in the Privileged Access Manager or native OS database.
editgrp	eg	AC and native	*Adds a new group to, or changes existing group settings in, the Privileged Access Manager or native OS database.
editres	er	AC and nt	*Adds a new resource record to, or changes an existing resource record in, the Privileged Access Manager or native OS database.
editres config		config	Lists the configuration settings in the source you specify.
editusr	eu	AC and native	*Adds a new user to, or changes an existing user in, the Privileged Access Manager or native OS database.

editxgrp	exg	AC	Adds a new enterprise group or changes existing enterprise group properties, in the Privileged Access Manager database.
editxusr	exu	AC	Adds a new enterprise user or changes existing enterprise user properties, in the Privileged Access Manager database.
end_transaction		AC	Completes the start_transaction command for Dual Control PMDB processes.
environment	env	all	Sets the security environment selang is operating on.
find	f	AC and native	Lists the classes in the environment or the records in a class.
findpmd		pmd	Lists all PMDBs on the computer.
find config		config	Lists sources of configuration settings (ini files or registry entries) you can manage on this host.
find file		native	Lists system files.
find xgroup		nt	Lists the names of enterprise groups in the current or trusted domains.
find xuser		nt	Lists the names of enterprise users in the current or trusted domains.
get dbexport		AC	Retrieves the rules that were exported from a Privileged Access Manager or PMD database.
get devcalc		AC	Retrieves policy deviation calculation results.
help		all	Displays selang help.
history		all	Displays the commands issued previously in the session.
hosts		all	Shows or sets the host to which selang commands are sent.
join	j	AC and native	*Joins a user to a group.
join-	j-	AC and native	*Removes a user from a group.
joinx	jx	AC	Joins an enterprise user to a group
joinx-	jx-	AC	Removes an enterprise user from a group.
list		AC and native	An alias of the <i>find</i> command.



listpmd		pmd	Lists information about the PMDB and its subscribers, update file, and error log.
newfile	nf	AC	Adds the definition of a file record in the Privileged Access Manager database.
newgrp	ng	AC and native	*Adds a new group to the Privileged Access Manager or native OS database.
newres	nr	AC and nt	*Adds a new resource record to the Privileged Access Manager or native OS database.
newusr	nu	AC and native	*Adds a new internal user to the Privileged Access Manager or native OS database.
newxgrp	nxg	AC	Adds a new enterprise group to the Privileged Access Manager database.
newxusr	nxu	AC	Adds a new enterprise user to the Privileged Access Manager database.
pmd		pmd	Clears the Policy Model error log, updates the subscriber list, releases subscribers, starts and stops the Policy Model service, truncates the update file, and reloads the initialization files.
rename		AC	Renames an object in the database.
restorepmd		pmd	Restores a PMDB on a local host.
rmfile	rf	AC	Removes a file resource record from the Privileged Access Manager database.
rmgrp	rg	AC and native	*Removes a group from the Privileged Access Manager or native OS database.
rmres	rr	AC and nt	*Removes a resource record from the Privileged Access Manager or native Windows database.
rmusr	ru	AC and native	*Removes a user from the Privileged Access Manager or native OS database.
rmxgrp	rxg	AC	Removes an enterprise group from the Privileged Access Manager database.
rmxusr	rxu	AC	Removes an enterprise user from Privileged Access Manager
ruler		AC and native	Sets the properties that display when a show command is executed.

search		AC and native	An alias of the <i>find</i> command.
setoptions	so	AC and nt	*Sets or displays the global options that control the behavior of the database.
showfile	sf	AC and native	*Lists the properties of file records in the Privileged Access Manager or native OS database.
showgrp	sg	AC and native	*Lists the properties of group records in the Privileged Access Manager or native OS database.
showres	sr	AC and nt	*Lists the properties of records in the Privileged Access Manager or native Windows database.
showres config		config	Lists the configuration settings in the source you specify.
showusr	su	AC and native	*Lists the properties of user records in the Privileged Access Manager database or the native OS database.
showxusr	sxu	AC	Lists the properties of enterprise user records in Privileged Access Manager.
source		<i>all</i>	Executes the commands in a specified file.
start dbexport		AC	Exports a Privileged Access Manager or PMD database.
start devcalc		AC	Triggers a policy deviation calculation.
start_transaction		AC	Starts recording a file that contains an unprocessed transaction for Dual Control PMDB processes, with one or more commands.
subs		pmd	Adds a subscriber to a parent PMDB or subscribes a database to a parent PMDB.
subspmd		pmd	Changes the parent of the database in the host to which you are connected.
unalias		AC and unix	Removes aliases for selang commands and properties.
undeploy		AC	An alias of the deploy-command.
unsubs		pmd	Removes subscribers from the subscriber list of a PMDB.
xaudit		nt	Sets auditing criteria and begins logging access events.
xaudit-		nt	Removes auditing criteria and stops logging access events.

**NOTE**

The native environment conforms to the rules of either the Windows (nt) or UNIX environments, depending on the operating system of the host to which you are connected.

## selang Commands in the PAM SC Environment

This section contains a complete alphabetic reference to all the selang commands that operate on the Privileged Access Manager database (commands in the AC environment).

Use the table of contents to access the topics in this section.

### alias Command Define selang Aliases

#### Valid on UNIX hosts

Use the alias command to list or define aliases for selang commands and properties. Any user can use the alias command.

**NOTE**

You can build a set of aliases to use in all selang sessions by defining those aliases in a startup file and using the *selang -r* command.

This command has the following format:

```
alias [aliasName [aliasValue]]
```

- *aliasName*  
(Optional) Defines the name you want to use as alias.  
If this option is not specified, the alias command lists all defined aliases.
- *aliasValue*  
(Optional) Defines the meaning that the selang command shell should associate with *aliasName*.  
If this option is not specified, the alias command displays the value of the specified alias.  
You can also include up to ten variables in *aliasValue* (\$0 to \$9). If *aliasValue* contains variables, you must replace each variable with the proper value in parentheses when invoking the alias.

#### Example: Use a Variable to Ease the Creation of New Administrators

To create an alias that makes adding new administrators to the database easier, enter the following command:

```
alias newadm newusr ($0) admin
```

To use this alias, simply add the names of the new administrators in brackets. For example:

```
newadm(Terri)
```

This adds a user called Terri to the database. Terri is given the ADMIN attribute which is required for administering the database. This is the same as entering the following command:

```
newusr Terri admin
```

#### Example: Simplify Property Names

To create an alias that replaces the property name *access* with the shortened alias *acc*, enter the following command:

```
alias acc access
```

You can now enter the following to use this alias:

```
authorize file x uid(y) acc(z)
```

### Example: Use Aliases in Context

Aliases are not simply expanded variables; they are only interpreted in a context where a command name or a property name should be specified. For example, define the alias:

```
alias newterm newres terminal
```

Then issue the following command:

```
newterm newterm owner(nobody)
```

The first newterm string is replaced but not the second as the context requires the second instance of the string to be a terminal name. This is the same as entering the following command:

```
newres terminal newterm owner(nobody)
```

## authorize Command Set Access Authorities on a Resource

### Valid in the AC environment

Use the authorize command to change accessors' access authorities to a resource.

This command modifies an access control list associated with a resource. It changes only one entry in an access control list at a time.

When an accessor attempts to access a resource, Privileged Access Manager checks the appropriate access control lists to determine the access authority. These access control lists include those that are in the resource record, and can also include access control lists in resource group records. If an accessor is denied access authority in any NACL that covers the resource, the authority is denied, even if the authority is granted in another ACL.

#### NOTE

The owner of a resource always has all access authorities to the resource. If you want to change the access authority of the user who is the owner, change the resource to have a different owner, for example, the user nobody.

#### NOTE

This command also exists in the Windows environment, but operates differently there.

To use the authorize command, you need sufficient authority, which means that one or more of the following must be true:

- You have the ADMIN attribute.
- You have the GROUP-ADMIN attribute for a resource group of which the resource is a member.
- You are the owner of the resource.
- You have modify access authority in the ADMIN class record that corresponds to the resource.

The authorize command has different forms for different sets of classes. These sets are:

- TCP
- HOST, GHOST, HOSTNET, and HOSTNP
- All other classes

This command has the following format for the TCP class:

```
{authorize|auth} TCP tcpServiceName \
[{access|deniedaccess} {accessType}] \
{[ghost(ghostName [,ghostName]...)] | \
[host(hostName [,hostName]...)] | \
[hostnet(hostNetName [,hostNetName]...)] | \
[hostnp(hostNamePattern [,hostNamePattern]...)]} \
```

```
[[gid|uid|xgid|xuid}{accessor [,accessor]...]] ...
```

This command has the following format for the HOST, GHOST, HOSTNET, and HOSTNP classes:

```
{authorize|auth} {HOST|GHOST|HOSTNET|HOSTNP} stationName
[{access|deniedaccess} (accessType)] \
service({serviceName|serviceNumber|serviceNumberRange})
```

This command has the following format for all other classes:

```
{authorize|auth} classNameresourceName \
[{access|deniedaccess} (accessType)] \
[calendar(calendarName)] \
[{unix|nt}]\
[via (pgm ( program [,program]...))] \
{ gid | uid | xgid | xuid}{accessor [,accessor...]} ...
```

- **access (*accessType*)**  
Defines the access authority entry in the resource ACL access control list. This ACL specifies which access authorities are granted to accessors.
    - **accessType**  
Defines the access type in the resource ACL, for example, read or write.
- NOTE**  
If you omit both the `access(accessType)` and the `deniedaccess(accessType)` options to the `authorize` command, Privileged Access Manager assigns the access that is specified by the implicit access property of the record in the UACC class for the class of resource (for example in the UACC file record if the resource is a file).
- **calendar(*calendarName*)**  
Specifies the calendar to use for determining access authority.
  - **className**  
Defines the class to which *resourceName* belongs.
  - **deniedaccess(*accessType*)**  
Changes the access authority in the resource NACL. The NACL specifies which access types are denied to accessors.
    - **accessType**  
Specifies the access type to be denied, for example, read, or write.
  - **gid (*accessor* [,*accessor*...])**  
Defines one or more internal groups for whom you want to set the access authority.
  - **ghost(*ghostName* [,*ghostName*]...)**  
Defines one or more group hosts for which you want to set access authority to the TCP/IP service.
  - **host(*hostName* [,*hostName*]...)**  
Defines one or more hosts for which you want to set access authority to the TCP/IP service.
  - **hostnet(*hostNetName* [,*hostNetName*]...)**  
Defines one or more HOSTNET records for which you want to set access authority to the TCP/IP service.
  - **hostnp(*hostNamePattern* [,*hostNamePattern*]...)**  
Defines one or more HOSTNP records for which you want to set access authority to the TCP/IP service.
  - **nt**  
Specifies whether to add values to the system ACLs in Windows.  
Valid for the FILE class only.
  - **resourceName**  
Defines the resource record whose access control list is being modified.
  - **service(*serviceName*|*serviceNumber*|*serviceNumberRange*)**  
Defines the services the local host is permitted to provide to the remote host or hosts.  
*serviceNumber* |*serviceNumberRange*

Defines the service number or range.

Specify a range as two integers separated by a -(hyphen), for example, 1-99.

**Limits:** An integer in the range 0 to 65535.

- **stationName**

Specifies the record name within the indicated class, as follows:

- **HOST:** Name of single station.
- **GHOST:** Name of a group of hosts as defined in the database by the ghostcommand.
- **HOSTNET:** Name of a group of hosts as defined by a set of mask and match values for the IP address.
- **HOSTNP:** Name of a group of hosts as defined by a name pattern.

For hosts that cannot be resolved, specify the IP address range in IPv4 or IPv6 format.

- **tcpServiceName**

Specifies the Privileged Access Manager TCP service record whose access authority you are setting.

- **uid (accessor [,accessor...])**

Defines one or more internal users for whom you want to set the access authority.

You can use \* to represent all internal users.

- **unix**

Specifies whether to add values to the system ACLs in UNIX.

Valid only on UNIX environments that support ACLs, and only for records in the FILE class.

- **via(pgm(programName [,programName]...))**

Defines one or more programs for conditional program access. The via parameter specifies an entry in the PACL of the resource. *programName* specifies a program that can access the resource. *programName* can contain wildcard characters. If a program matches several entries in a PACL, the entry with the longest non-wildcard match takes precedence.

If *programName* specifies a program or shell script that is not defined in the PROGRAM class, Privileged Access Manager automatically creates a PROGRAM record to protect it.

- **xgid (accessor [,accessor...])**

Defines one or more enterprise groups for whom you want to set the access authority.

- **xuid (accessor [,accessor...])**

Defines one or more enterprise users for whom you want to set the access authority.

### Example: Authorize Angela to Read a File

The following selang command authorizes enterprise user Angela to read the file protected by the FILE resource /projects/secrets:

```
auth FILE /projects/secrets xuid(Angela) access(read)
```

### Example: Authorize Only Angela to Read a File

The following selang commands authorize enterprise user Angela, but nobody else, to read the file protected by the FILE resource /projects/secrets:

```
auth FILE /projects/secrets xuid(Angela) access(read)
auth FILE /projects/secrets defaccess (none)
chres FILE /projects/secrets owner(nobody)
```

#### NOTE

On UNIX, if you want *read* privileges to control whether users can perform operations that obtain information about the file (such as ls -l), set the STAT\_intercept configuration setting to 1. For more information, see the *Reference Guide*.

### Example: Authorize All Users in a Group to Log in to a Terminal

The following selang command authorizes all members of the enterprise group RESEARCH to log in to the terminal protected by the TERMINAL resource *tty10*:

```
auth TERMINAL tty10 xgid(RESEARCH) access(read)
```

### Example: Authorize Joe to Back up Files

The following selang command authorizes enterprise user Joe to back up the files protected by the GFILE resource `secret_files`:

```
auth GFILE secret_files xuid(Joe) \
via(pgm(/bin/backup)) access(read)
```

For a Windows endpoint, an equivalent command is as follows:

```
auth GFILE secret_files xuid(Joe) \
via(pgm(C:\WINDOWS\system32\ntbackup.exe)) access(read)
```

These commands only have an effect if the Joe's access authority is not determined by the ACL or NACL of the resource.

## authorize- Command Remove Access Authorities from a Resource

### Valid in the AC environment

Use the `authorize-` command to remove accessors from the access control lists (ACLs) of a resource.

#### NOTE

This command also exists in the native Windows environment but operates differently there.

#### NOTE

You need the same access authority to use the `authorize-` command as you do to use the `authorize` command.

The `authorize-` command has different formats for different sets of classes. These sets are:

- TCP
- HOST, GHOST, HOSTNET, and HOSTNP
- All other classes

This command has the following format for the TCP class:

```
{authorize-|auth-} TCP tcpServiceName \
{gid |uid |xgid |xuid } (accessorName [,accessorName]...)\
[host(hostName [,hostName]...)] \
[ghost(ghostName [,ghostname]...)] \
[hostnet(hostNetName [,hostNetName]...)] \
[hostnp(hostNamePattern [,hostNamePattern]...)]
```

This command has the following format for the HOST, GHOST, HOSTNET, and HOSTNP classes:

```
{authorize-|auth-} classNameestationName \
service({serviceName | serviceNumber |serviceNumberRange})
```

This command has the following format for all remaining classes:

```
{authorize-|auth-} classNameresourceName \
[{access-|deniedaccess-}]\
[calendar(calendarName)] \
{gid |uid |xgid |xuid } (accessorName [,accessorName]...)
```

- **access-**  
Specifies that the command should remove accessors from the resource ACL (which grants access authorities), rather than from the NACL.

If neither `access-` or `deniedaccess-` are specified, the command removes the accessors from both ACLs.

- **calendar**(*calendarName*)  
Removes the calendar specified for determining access authority.
- **className**  
Specifies the name of the class to which *resourceName* belongs.
- **deniedaccess-**  
Specifies that the command should remove accessors from the resource NACL (which denies access authority), rather than from the ACL.
- **gid** (*accessor* [,*accessor*]...)  
Defines one or more internal groups whose entries are to be removed. Separate each *accessor* with a comma or space.
- **ghost**(*ghostName*)  
Specifies the name of an object in class GHOST.
- **host**(*hostName*)  
Specifies the name of an object in class HOST.
- **hostnet**(*hostNetName*)  
Specifies the name of an object in class HOSTNET.
- **hostnp**(*hostNamePattern*)  
Specifies a pattern defined in class HOSTNP.
- **nt**  
Specifies whether to remove values from the system ACLs in Windows.  
Valid for the FILE class only.
- **resourceName**  
Specifies the name of the resource record whose access control list is being modified. Specify only one resource record.
- **service**(*serviceName*|*serviceNumber*|*serviceNumberRange*)  
Defines the services you want to remove from an ACL.
  - **stationName**  
Specifies the record name within the indicated class, as follows:
    - **HOSTName** of single station.
    - **GHOSTName** of a group of hosts as defined in the database by the `ghostcommand`.
    - **HOSTNETName** of a group of hosts as defined by a set of mask and match values for the IP address.
    - **HOSTNPName** of a group of hosts as defined by a name pattern.
 For hosts that cannot be resolved, specify the IP address range.
  - serviceNumber** |**serviceNumberRange**  
Defines the service number or range.  
Specify the range as two integers separated by a -(hyphen), for example, 1-99.  
**Limits:** An integer in the range 0 to 65535
- **uid** (*accessor* [,*accessor*]...)  
Defines one or more internal users whose entries are to be removed. Separate each *accessor* with a comma or space.  
You can use `uid(*)` to specify all internal users.
- **unix**  
Specifies whether to remove add from the system ACLs in UNIX.  
Valid only on UNIX environments that support ACLs, and only for records in the FILE class.
- **xgid** (*accessor* [,*accessor*]...)  
Defines one or more enterprise users whose entries are to be removed. Separate each *accessorName* with a comma or space.
- **xuid** (*accessor* [,*accessor*]...)  
Defines one or more enterprise groups whose entries are to be removed. Separate each *accessor* with a comma or space.



### Example: Remove a group authority to access a file

The following command removes the group `research` from both the ACL and NACL of the file covered by the resource `/products/new`:

```
auth- FILE /products/new xgid(research)
```

The `research` group now has the default access to the file.

## check Command Determine a User's Access Authority

### Valid in the AC environment

Use the `check` command to determine if a user has access privileges to a particular resource. The command checks access according to the resource's ACL and default access property. However, it does not support PACLS; that is, it does not indicate whether the user can access a resource using a specific program.

#### NOTE

This command is not available when `seos` is down. For more information about PACLS, see the *Endpoint Administration Guide* for your OS.

To use this command you must have sufficient authority over the resource, as defined by any of the following conditions:

- The process running the command has the `SERVER` attribute.
- You have the `ADMIN` attribute.

This command has the following format:

```
check className resourceName uid(userName) access(authority)
```

- `access(authority)`  
Defines the access authority to be checked for the accessor identified by the `uid` parameter.  
Valid values depend on the resource being checked.
- `className`  
Defines the name of the class to which `resourceName` belongs.
- `resourceName`  
Defines the name of the resource record.
- `uid(userName)`  
Defines the name of the Privileged Access Manager user whose authority to access `resourceName` is to be verified.

### Example: Determine whether a user has access to a resource

To determine whether user `Alain` has write access to the resource `testfile` of class `file`, enter the following command:

```
check FILE /testfile uid(Alain) access(w)
```

The following sample output of this command indicates that user `Alain` has write access to the defined file because `Alain` is the resource's owner:

```
Access to FILE /testfile GRANTED
Stage: Resource OWNER check
```

## checklogin Command Determine Login Information

### Valid in the AC environment

Use the `checklogin` command to determine a user's login privileges, whether a password check is needed, and whether a terminal access check is needed.

**NOTE**

This command is not available when seos is down.

To use this command you must have sufficient authority over the resource, as defined by any of the following conditions:

- The process running the command has the SERVER attribute.
- You have the ADMIN attribute.

This command has the following format:

```
checklogin userName [password(password)] [terminal(terminalName)]
```

- **password(*password*)**  
(Optional) Defines the password that Privileged Access Manager checks against the operating system password and the database, if password checking is enabled.
- **userName**  
Defines the name of the user whose right to login is being verified.
- **terminal(*terminalName*)**  
(Optional) Defines the terminal that Privileged Access Manager checks to determine if a user has login privileges from it.

**Example: Determine whether user has login privileges**

To determine whether user Frank has login privileges to the *localhost* from terminal *mutra*, enter the following command:

```
checklogin Frank terminal(mutra)
```

The following output of the command, indicates that user Frank can login from terminal *mutra* to host *winsome* (localhost):

```
Login by USER frank to host winsome is GRANTED
Stage: Resource class global universal access
```

To verify user Frank's password, enter the following command:

```
checklogin frank password(111) terminal(localhost)
```

To verify user Frank's password against the one in the Privileged Access Manager database, enter the following commands:

```
so class+(PASSWORD) (localhost)
checklogin frank password(moonshine) terminal(tack)
```

The *so* command above enables password checking.

**checkpwd Command Check a Password for Compliance****Valid in the AC environment**

Use the *checkpwd* command to check a user's password for compliance with password rules. This check does not change the password.

To use this command you must be a superuser with the ADMIN attribute.

A new password is accepted or rejected according to Privileged Access Manager password rules:

- If a new password is accepted, the following success message displays:  
Changing *userName*'s password is permitted.
- If a new password is rejected, the following fail message displays:  
Changing *userName*'s password is denied.  
*denied\_reason*

Where *denied\_reason* is the actual password rule that did not pass.

For example:

```
Changing JDoe's password is denied.
Too few lowercase letters in password.
```

Only the first rule that the password fails appears in the *denied\_reason*. If, for example, a password is too short, *and* the password has too few capital letters, only *Password is too short* appears.

#### NOTE

This command is not available when seos is down. For more information about password rules, see the *Endpoint Administration Guide* for your OS.

This command has the following format:

```
checkpwd userName password(newPassword)
```

- *userName*  
Specifies the name of the Privileged Access Manager user whose new password you want to check.
- *password(newPassword)*  
Specifies the password you want to check.

## chfile Command Modify File Records

### Valid in the AC environment

Use the *chfile*, *editfile*, and *newfile* commands to work with records in the FILE class. These commands are identical in structure and only vary in the following way:

- The *chfile* command *modifies* one or more records in the FILE class.
- The *editfile* command *creates or modifies* one or more records in the FILE class.
- The *newfile* command *creates* one or more records in the FILE class.

#### NOTE

This command also exists in the native environment but operates differently.

To add or change a record for a file belonging to the FILE class, you must have sufficient authority over the file. Privileged Access Manager makes the following checks until one of the following conditions is met:

1. You have the ADMIN attribute.
2. The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
3. When changing a record, that you are its owner.
4. You have CREATE (for *newfile* or *editfile*) or MODIFY (for *chfile*) access authority in the ACL of the FILE record in the ADMIN class.
5. That you are the owner of the file (when defining a file to Privileged Access Manager that exists in the native OS), if the token *use\_unix\_file\_owner* in the *seos.ini* file is set to yes.

```
{{chfile|cf}}{{editfile|ef}}{{newfile|nf}} filename... \
[audit{none|all|success|failure}] \
[category[-](categoryName)] \
[comment(string)|comment-] \
[defaccess(accessAuthority)] \
[label(labelName)|label-] \
[level(number)|level-] \
[notify(mailAddress)|notify-] \
[gowner(groupName)] \
[owner({userName|groupName})] \
```

```
[restrictions( \[days({anyday|weekdays|{[mon] [tue] [wed] \ [thu] [fri] [sat] [sun]}})] \[time({anytime|
startTime:endTime}) \
|restrictions-] \
[warning|warning-]
```

- **audit{none|all|success|failure}**

Specifies which access events Privileged Access Manager logs:

- **all** - Both authorized accesses and detected unauthorized access attempts.
- **failure** - Detected unauthorized access attempts. This is the default value.
- **none** - Does not write any records in the log file.
- **success** - Authorized accesses to the resource.

**NOTE**

To use the audit parameter, you must have the AUDITOR attribute.

- **category(categoryName)**

Defines a space- or comma-separated list of security category records (defined in the CATEGORY class) to assign to the file.

If you specify the category parameter when the CATEGORY class is not active, Privileged Access Manager updates the definition of the file in the database; however, the updated category assignment has no effect until the CATEGORY class is activated again.

**NOTE**

For more information about security category checking, see the *Endpoint Administration Guide* for your OS.

- **category-(categoryName)**

Deletes one or more security categories from the resource record. When removing more than one security category, separate the security category names with a space or a comma.

The specified security categories are deleted from the resource record, regardless of whether the CATEGORY class is active.

**NOTE**

This parameter is only valid when modifying a record.

- **comment(string)**

Adds an alphanumeric string to the group record. If you previously added a comment string to the group record, the new string specified here replaces the existing string.

**Format:** Up to 255 characters including double bytes and special characters. If the string contains any blanks, enclose the string in quotation marks.

- **comment-**

Deletes the comment string from the file record.

**NOTE**

This parameter is only valid when modifying a record.

- **defaccess(accessAuthority)**

Specifies the default access authority for the file. The default access authority is the authority granted to any accessor that requests access to the file, but that is not in the access control lists of the file. The default access is also applied to users who are not defined in the database.

- **fileName**

Defines the name of the file record. At least one file name must be specified.

If you are adding or changing a record in class FILE using a generic file name, use the wildcard expressions permitted in selang. When defining or changing more than one record, enclose the list of file names in parentheses and separate the file names with a space or a comma.

**NOTE**

If more than one file name is specified, Privileged Access Manager processes each file record independently in accordance with the specified parameters. If an error occurs while processing a file, Privileged Access Manager issues a message and continues processing with the next file in the list.

- **gowner(*groupName*)**  
Assigns a Privileged Access Manager group as the owner of the file record. The group owner of the file record has unrestricted access to the file, provided the group owner's security level, security label, and security category authorities are sufficient to allow access to the file. The group owner of the file is always permitted to update and delete the file record.
- **label(*labelName*)**  
Assigns to the file a security label defined in the SECLABEL class. A security label represents an association between a particular security level and zero or more security categories. If the resource record currently contains a security label, the security label specified here replaces the current security label.

**NOTE**

For more information about security label checking, see the *Endpoint Administration Guide* for your OS.

- **label-**  
Deletes the security label defined in the file record.

**NOTE**

This parameter is only valid when modifying a record.

- **level(*number*)**  
Assigns a security level to the resource record. Enter a positive integer between 1 and 255. If a security level was previously assigned to the resource record, the new value replaces the existing value.

**NOTE**

For more information about security level checking, see the *Endpoint Administration Guide* for your OS.

- **level-**  
Stops Privileged Access Manager from performing security level checking for the resource.

**NOTE**

This parameter is only valid when modifying a record.

- **notify(*mailAddress*)**  
Instructs Privileged Access Manager to send notification messages whenever the file represented by the resource record is successfully accessed. Enter a user name, an email address of a user, or the email address of a mail group if an alias is specified.  
Notification takes place only when the Log Routing System is active. The notification messages are sent either to the screen or to the mailbox of the users, depending on the setup of the Log Routing System.  
Each time a notification message is sent, an audit record is written in the audit log.  
The recipient of notify messages should log in frequently to respond to the unauthorized access attempts described in each message.  
**Limit:** 30 characters.

**NOTE**

For information about filtering and viewing audit records, see the *Endpoint Administration Guide* for your OS.

- **notify-**  
Specifies that no one is notified when Privileged Access Manager grants access to the file represented by the record.

**NOTE**

This parameter is only valid when modifying a record.

- **owner(*Name*)**

Assigns a Privileged Access Manager user or group as the owner of the file record. The owner of the file record has unrestricted access to the file, provided the owner's security level, security label, and security category authorities are sufficient to allow access to the file. The owner of the file is always permitted to update and delete the file record.

- **restrictions(days(*dayData*) time(*timeData*))**  
Specifies the days of the week and the hours in the day when the file is accessible to users.  
If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users are allowed to access the system only during the specified time period on the specified days.
  - **days( *dayData* )**  
Specifies the days on which users can access the file. The days argument takes the following sub-arguments:
    - a. **anyday** - Gives access to the file on any day.
    - b. **weekdays** - Gives access to the resource only on weekdays-Monday through Friday.
    - c. **mon tue wed thu fri sat sun** - Gives access to the resource only on the specified days. You can specify the days in any order. If more than one day is specified, separate the days with a space or a comma.
  - **time(*timeData*)**  
Specifies the period during which users can access the file. The time argument takes the following sub-arguments:
    - a. **anytime** - Gives access to the resource at any time of the day.
    - b. **startTime : endTime**-Gives access to the resource only during the specified period. The format of both *startTime* and *endTime* is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. *StartTime* must be less than *endTime*, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time(1100:2000).
- **restrictions-**  
Deletes any restrictions that limit the ability to access the file.
 

**NOTE**  
This parameter is only valid when modifying a record.
- **warning**

**NOTE**  
Puts the file into Warning mode.
- **warning-**  
Takes the file out of Warning mode.

### Example: Restrict Access to a File to All but the Superuser

To restrict access to the `/etc/passwd` file to READ access to all users except the superuser, enter the following command:

```
chfile /etc/passwd defaccess(read) owner(root)
```

The following must be true:

- You have the ADMIN attribute.
- The record `/etc/passwd` is defined in the database.
- There are no entries in the ACL of the record `/etc/passwd`.

### Example: Restrict Access to a File by Time

To prevent access to the `/home/bob/secrets` file and let the owner access the file only on weekdays between 08:00 and 18:00, enter the following command:

```
newfile /home/bob/secrets defac(none) restrictions(d(weekdays) t(0800:1800))
```

The following must be true:

- You have the ADMIN attribute.
- Bob is a Privileged Access Manager user and is the owner of the /home/ bob/secretsrecord in the FILE class.

### Example: Prevent Access to Your Home Directory

To prevent all other users from accessing any file in your home directory (/home/bob), enter the following command on UNIX:

```
newfile /home/bob/* defaccess(none)
```

You can do the same on Windows using the following command:

```
newfile %userprofile%\* defaccess(none)
```

The following must be true:

- You are defined to Privileged Access Manager.
- You are the native owner of the file.

## ch x grp Command Change Group Properties

### Valid in the AC environment

Use the commands chgrp, chxgrp, editgrp, editxgrp, newgrp, and newxgrp to change the properties of groups, and to create the groups in the Privileged Access Manager database if necessary.

These commands all have synonyms, as follows:

- chgrpcg
- chxgrpcxg
- editgrpeg
- editxgrpexg
- newgrpng
- newxgrpnxg

These commands are identical in structure, and vary only in their scope, in the following ways:

- The chgrp, editgrp, and newgrp commands work with records in the GROUP class. These let you create or modify Privileged Access Manager groups without reference to the enterprise user store. The differences between these commands are as follows:
  - The chgrp command *modifies* one or more records in the GROUP class.
  - The editgrp command *creates or modifies* one or more records in the GROUP class.
  - The newgrp command *creates* one or more records in the GROUP class.

#### NOTE

These commands also exist in the native environment but operate differently there.

- The chxgrp, editxgrp and newxgrp commands work on records in the XGROUP class. These let you create or modify Privileged Access Manager groups that are defined in the enterprise user store. The differences between them are as follows:
  - The chxgrp command *modifies* one or more records in the XGROUP class.
  - The editxgrp command *creates or modifies* one or more records in the XGROUP class.
  - The newxgrp command *creates* one or more records in the XGROUP class.

### Authorization Required

To create a new Privileged Access Manager group, at least one of the following conditions must be true:

- You have the ADMIN attribute.
- You are assigned the CREATE authority in the access control list of the GROUP or XGROUP record in the ADMIN class.

To add or modify a group, at least one of the following conditions must be true:

- You have the ADMIN attribute.
- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group.
- You are assigned the MODIFY (for ch[x]grp) or CREATE (for edit[x]grp) authority in the access control list of the GROUP or XGROUP record in the ADMIN class.

```
{ {chgrp|cg} | {chxgrp|cxg} | {editgrp|eg} | {editxgrp|exg} | {newgrp|ng} | {newxgrp|nxg} } groupName ...
[{admin | admin-}] \
[audit(none|all|success|failure|loginsuccess|loginfail|trace|interactive)|audit-] \
[{auditor | auditor-}] \
[comment(string)|comment-] \
[expire[(mm/dd/yy[yy[ @hh:mm]])]|expire-] \
[gowner(groupName)] \
[homedir(fullPath|nohomedir)] \
[inactive(numInactiveDays)|inactive-] \
[maxlogins(maximumNumberOfLogins)|maxlogins-] \
[mem(groupName)|mem+(groupName)|mem-(groupName)] \
[name('fullName')] \
[nt[(comment(comment))]]
[{operator | operator-}] \
[owner(userName|groupName)] \
[parent(groupName)|parent-] \
[password( \ [history(numberStoredPasswords)|history-] \ [interval(maximumPasswordChangeInterval)|interval-]
 \ [min_life(minimumPasswordChangeInterval)|min_life-] \ [rules( \ [alpha(minimumAlphaCharacters)] \
 [alphanum(minimumAlphanumericCharacters)] \ [bidirectional|bidirectional-] \ [grace(numberOfGraceLogins)] \
 [min_len(minimumPasswordLength)] \ [max_len(maximumPasswordLength)] \ [lowercase(minimumLowercaseCharacters)]
 \ [max_rep(maxRepetitiveCharacters)] \ [namechk|namechk-] \ [numeric(minimumNumericCharacters)] \ [oldpwchk|
oldpwchk-] \ [special(minimumSpecialCharacters)] \ [uppercase(minimumUppercaseCharacters)] \ [use_dbdict|
use_dbdict-] \ )|rules-] \ )] \
[pmdb(PolicyModelName)|pmdb-] \
[{pwmanager | pwmanager-}] \
[restrictions( \ [days({anyday|weekdays|{[mon] [tue] [wed] \ [thu] [fri] [sat] [sun]}})] \ [time(anytime|
startTime:endTime)] \
|restrictions-] \
[resume[(mm/dd/yy[yy] [ @hh:mm]])]|resume-] \
[{server | server-}] \
[shellprog(fullPath)] \
[supgroup(superiorGroup)|supgroup-] \
[suspend[(mm/dd/yy[yy] [ @hh:mm]])]|suspend-] \
[unix[( \ [appl(quotedString)] \ [groupid(groupidNumber)] \ [userlist(userName...)] \
)]] \
```

To remove any record property where the property is defined by a string, type the property followed immediately by either - (minus sign), or () (empty parenthesis).

#### NOTE

Some parameters are relevant only when a group functions as a profile group. A profile group cannot be an enterprise group.



- **admin**  
Assigns the ADMIN attribute to the group. A user who is a member of a group with the ADMIN attribute is allowed to issue all selang commands with all parameters except the audit parameter. You must have the ADMIN attribute to use the admin parameter.
- **admin-**  
Removes the ADMIN attribute from the group. (Privileged Access Manager ensures that at least one user has the ADMIN attribute.)  
You cannot use this parameter with the new[x]grp command.
- **audit(mode)**  
Turns on the trace audit for this command. The audit modes are: none, all, success, failure, loginsuccess, loginfail, trace, interactive.
- **audit-**  
Turns off the trace audit for this command.
- **auditor**  
Assigns the AUDITOR attribute to the group. A user who is a member of a group with the AUDITOR attribute can audit the use of system resources and is able to control the logging of detected accesses to any Privileged Access Manager-protected resource during Privileged Access Manager authorization checking and accesses to the database. See the *Endpoint Administration Guide* for your OS for more information on the authorities granted to a user with the AUDITOR attribute.
- **auditor-**  
Removes the AUDITOR attribute from the group record.  
You cannot use this parameter with the new[x]grp command.
- **comment(string)**  
Adds to the group record a comment string of up to 255 alphanumeric characters (single-byte). If the string contains spaces, enclose the entire string in single quotation marks. The string replaces any existing string that you added previously.

**NOTE**

In German, only 128 characters are recorded.

- **comment-**  
Deletes the comment string, if any, from the group record. Use this parameter only with the chgrp or editgrp command.
- **expire(date)**  
Sets the date on which the accounts of the group members expire. If you do not specify a date, the user accounts expire immediately, provided the users are not currently logged in. If the users are logged in, the accounts expire when the users log out. This parameter applies only to profile groups.  
Specify the expiration date, and optional time, in the following format: *mm/dd/yy [yy][@HH:MM]*. Year can be either 2 or 4 digits.

**NOTE**

You cannot enable expired user records by specifying the resume parameter with a resume date. Use the expire- parameter to enable expired user records.

- **expire-**  
For the newgrp command, defines user accounts that do not have an expiration date. For the chgrp and editgrp commands, removes the expiration date from the user accounts. This parameter applies only to profile groups.
- **gowner(groupName)**  
Assigns a Privileged Access Manager user or group as the owner of the group record. When you specify more than one group name, enclose the names in parentheses and separate the group names with a space or a comma. If you add a group to the database and omit this parameter, you are the owner of the group record.
- **grace(numberOfGraceLogins)**  
Sets the maximum number of logins that are permitted before the users are suspended. The number of grace logins must be between 0 and 255. After the number of grace logins is reached, the users are denied access to the system

and must contact the system administrator to select a new password. If grace is set to zero, the users cannot log in. This parameter applies only to profile groups.

- **grace-**  
Deletes the grace login setting for the group. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **groupName**  
Specifies the name of the group you are creating or whose properties you are changing. For the command `new[x]grp`, each group name must be unique and must not currently exist in the database. However, a group and a user can share the same name.
- **history**  
Specifies the number of stored passwords. You can eliminate the history file with `history-`.
- **homedir(*fullPath*|nohomedir)**  
Specifies the full path of the users' home directories. If the path you specify ends with a slash, *groupName* is concatenated to the specified path. If you specify `nohomedir` then a home directory is not automatically set.
- **inactive(*numInactiveDays*)**  
Specifies the number of days that must pass before the system changes users to inactive status. When the number of days is reached, users cannot log in. This parameter applies only to profile groups.  
Enter a positive integer or zero for *numInactiveDays*. If inactive is set to zero, the effect is the same as using the `inactive-` parameter.

#### NOTE

In the user record, inactive users are not marked. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

- **inactive-**  
Changes the users' status from inactive to active. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **interval(*maximumPasswordChangeInterval*)**  
Sets the number of days that must pass after the password was set or changed before the system prompts the user for a new password. Enter a positive integer or zero. An interval of zero disables password interval checking for the group so that the password does not expire. The default set by the `setoptions` command is not used. Set an interval of zero only for users with low security requirements.  
When the specified number of days is reached, Privileged Access Manager informs the user that the current password has expired. The user can immediately renew the password or continue using the old password until the number of grace logins is reached. After the number of grace logins is reached, the user is denied access to the system and must contact the system administrator to select a new password. This parameter applies only to profile groups.
- **interval-**  
Cancels the password interval setting for the group. If canceled, any value in the user record is used. Otherwise, the default set by the `setoptions` command is used. Enter this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **maxlogins(*maximumNumberOfLogins*)**  
Sets the maximum number of terminals users can log in to at the same time. A value of 0 (zero) means that users can log in from any number of terminals concurrently. If this parameter is not specified, any value in the user record is used. Otherwise, the global maximum logins setting is used. This parameter applies only to profile groups.

#### NOTE

If `maxlogins` is set to 1, you cannot run `selang`. You must shut down Privileged Access Manager, change the `maxlogins` setting to greater than one, and start Privileged Access Manager again.

- **maxlogins-**  
Deletes the group's maximum login setting. If this parameter is not specified, any value in the user record is used. Otherwise, the global maximum logins setting is used. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **mem(*GroupName*) | mem+(*GroupName*)**

Adds members groups (or child groups) to the group in Privileged Access Manager. The member groups (*GroupName*) must already be defined in Privileged Access Manager. If you are adding more than one member group, separate the group names with a comma. If a group name contains a space, enclose it in quotation marks.

**Note:** To add users to a internal group, use the join[x] command.

This option applies to internal groups only.

- **mem-(*GroupName*)**  
Removes member groups from this group. The member groups (*GroupName*) must already be defined in Privileged Access Manager. If you are removing more than one member group, separate the group names with a comma. If a group name contains a space, enclose it in quotation marks.  
**Note:** To remove users from a internal group, use the join[x]- command.  
This option applies to internal groups only.
- **min\_life(*minimumPasswordChangeInterval*)**  
The minimum number of days that must pass before users are allowed to change the password again. This parameter applies only to profile groups.
- **min\_life-**  
Deletes the min\_life setting of a group. If this parameter is not specified and the min\_life parameter is set in a user record, the value in the user record is used. Otherwise, the global min\_life setting is used. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.
- **name(*fullname*)**  
Specifies the full name of the group. Enter an alphanumeric string of up to 47 characters. If the string contains any blanks, enclose the string in single quotation marks.
- **nt(*nt-group-attributes*)**  
(Windows only) Adds or changes the group definition in the local Windows system.
  - **comment('comment')**  
Adds a comment string to the native record. If you previously added a comment string to the record, the new string specified here replaces the existing string.  
*comment* is an alphanumeric string of up to 255 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **operator**  
Assigns the OPERATOR attribute to the group. A user who is a member of a group with the OPERATOR attribute can list all resource records in the database, and has read authority for all Privileged Access Manager defined files. A user who is a member of a group with this attribute can also use all the options of the secons command. See the *Reference Guide* for more information on the secons utility.
- **operator-**  
Removes the OPERATOR attribute from a group record.  
You cannot use this parameter with the new[x]grp command.
- **owner(*Name*)**  
Assigns a Privileged Access Manager user or group as the owner of the group record. If you are adding a group to the database and you omit this parameter, you are the owner. See the *Endpoint Administration Guide* for your OS for more information.
- **parent(*groupName*)**  
Assigns an existing Privileged Access Manager group as the parent group of the group record. See the *Endpoint Administration Guide* for your OS for more information on parent and child relationships.
- **parent-**  
Deletes the link between a group and its parent group. Use this parameter only with the chgrp or editgrp command.
- **password**  
Assigns a password to this group.
- **password-**  
Deletes the need for a password for this group.
- **pmdb(*PolicyModelName*)**

Specifies that when a user in the group changes a password with the utility `sepass`, the new password is propagated to the specified Policy Model. Enter the fully qualified name of the PMDB.

The password is not sent to the Policy Model defined in the `parent_pmd` or `passwd_pmd` token in the `[seos]` section of `seos.ini`. This parameter applies only to profile groups.

- **pmdb-**  
Removes the PMDB attribute from the group record. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **pwmanager**  
Assigns the PWMANAGER attribute to the group. A user who is a member of a group with this attribute can change the passwords of users in the database. See the *Endpoint Administration Guide* for your OS for more information.
- **pwmanager-**  
Removes the PWMANAGER attribute from the group record.  
You cannot use this parameter with the `new[x]grp` command.
- **restrictions(days(*dayData*) time(*timeData*))**  
Specifies the days of the week and the hours in the day when members of the group are allowed to log in to the system.  
Privileged Access Manager does not force a user off the system if the login period expires while the user is logged in. Also, the login restrictions do not apply to batch jobs; a user can run a background process at any time. This parameter applies only to profile groups.  
If you omit the `days` argument and specify the `time` argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit `time` and specify `days`, the day restriction applies to any time restriction already indicated in the record. If you specify both `days` and `time`, the members of the group are allowed to access the system only during the specified time period on the specified days.
  - **days( *dayData* )**  
Specifies the days on which users can log in to the system. The `days` argument takes the following sub-arguments:
    - a. **anyday**-Lets users log in on any day.
    - b. **weekdays**-Lets users log in only on weekdays-Monday through Friday.
    - c. **mon tue wed thu fri sat sun**-Lets users log in only on the specified days. You can specify the days in any order. If more than one day is specified, separate the days with a space or a comma.
  - **time( *timeData* )**  
Specifies the period during which users can log in to the system. The `time` argument takes the following sub-arguments:
    - a. **anytime**-Lets users log in at any time of the day.
    - b. **startTime : endTime**-Lets users log in only during the specified period. The format of both *startTime* and *endTime* is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. If *endTime* is a smaller number than *endTime*, the period is considered to extend across midnight. Otherwise, it is considered to take place on a single day.  
**Note:** Privileged Access Manager uses the time zone of the processor. If the user logs in at a terminal in a different time zone from the processor, you must take this into account.
- **restrictions-**  
Deletes any restrictions that limit the users' ability to log in to the system from the group record. If this parameter is not specified and the `restrictions` parameter is set in a user record, the value in the user record is used. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.
- **resume(*date*)**  
Enables user records that were disabled by specifying the `suspend` parameter. Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM]*.  
If you specify both the `suspend` parameter and the `resume` parameter, the resume date must fall after the suspend date. If you omit *date*, the user is enabled immediately on execution of the `chgrp` command. See the *Endpoint Administration Guide* for your OS for more information. This parameter applies only to profile groups.
- **resume-**

Erases the resume date, and time if used, from the group record. Consequently, the status of the users is changed from active (enabled) to suspended. Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.

- **rules**

Specifies rules for the password:

- `alpha(minimumAlphaCharacters)`  
Minimum number of alphabetic characters.
- `alphanum(minimumAlphanumericCharacters)`  
Minimum number of characters.
- **bidirectional|bidirectional-**  
Specifies whether to use bidirectional password encryption. If bidirectional password encryption is enabled, each new password is encrypted and can be decrypted back to clear text. This encryption gives a wider comparison between new passwords and old passwords (password history). When bidirectional encryption is disabled, one-way password history encryption is activated, and you cannot decrypt old passwords.

**NOTE**

You must set history to a value greater than 1 to use this feature.

**WARNING**

If you set the `seos.ini` file token "passwd\_format" ([passwd] section) to "NT", you must use the "native" option (rather than `unix`) when you create a user in `selang`. For example:

```
nu uSr_1026 native password(uSr_1026)
```

**WARNING**

Alternatively, make sure that you work in the native environment (rather than the `unix` one), as follows:

```
env native
chusr usr_1 password(mypassword)
```

- `min_len(minimumPasswordLength)`  
Minimum password length.
- `max_len(maximumPasswordLength)`  
Maximum password length.
- `lowercase(minimumLowercaseCharacters)`  
Minimum number of lowercase characters.
- `max_rep(maximumRepetitiveCharacters)`  
Maximum number of repeated characters.
- **namechk|namechk-**  
Check password against name.
- `numeric(minimumNumericCharacters)`  
Minimum number of numeric characters.
- **oldpwchk|oldpwchk-**  
Check password against old password.

**NOTE**

Valid only on Unix and Linux operating systems.

`special(minimumSpecialCharacters)`

Minimum number of special characters.

- `uppercase(minimumUppercaseCharacters)`  
Minimum number of uppercase characters.
- **use\_dbdict|use\_dbdict-**

Sets the password dictionary. `use_dbdict` sets the token to **db** and compares passwords against words in the Privileged Access Manager database. `use_dbdict-` sets the token to **file** and checks passwords against a file specified in the `seos.ini` file for UNIX or Windows registry for Windows.

## server

Sets the SERVER attribute on. If the current user is a member of a group with the SERVER attribute on, it allows a process running on behalf of the current user to ask for authorization for other users. See the *Endpoint Administration Guide* for your OS for more information.

## server-

Sets the SERVER attribute off.

You cannot use this parameter with the `new[x]grp` command.

## shellprog(fullPath)

Specifies the full path of the initial program or shell that is executed after the user invokes the login or su command. *FullPath* is a character string.

`supgroup(Group'sSuperiorGroup)`

Specifies a supergroup (or parent group).

`suspend(date)`

Disables user records, but leaves them defined in the database. Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM]*.

A user cannot use a suspended user account to log in to the system. If *date* is specified, the user records are suspended on the specified date. If *date* is omitted, the user records are suspended immediately upon execution of the `chgrp` command. This parameter applies only to profile groups.

`suspend-`

Erases the suspend date from the user records, changing the status of the users from disabled to active (enabled). Use this parameter only with the `chgrp` or `editgrp` command. This parameter applies only to profile groups.

`unix(groupidNumber)`

(UNIX only) Sets group attributes on UNIX or creates the group if it does not already exist.

The *groupidNumber* is a decimal number. You cannot specify a group ID of zero. If you omit the number, Privileged Access Manager finds the largest current group ID and sets the ID of the group to this number. Privileged Access Manager creates group ID numbers in the same way when adding or modifying more than one group at a time. The token `AllowedGidRange` in the `seos.ini` file may define certain unavailable numbers.

`userlist(userName)`

Assigns members to the group. *UserName* is the user name of one or more UNIX users. When assigning more than one user, separate the user names with a comma or a space. For the `chgrp` and `editgrp` commands, the member list specified here replaces any member list that is currently defined for the group.

## Examples

- The user Bob wants to change the parent group and owning group for the enterprise group Sales from ACCOUNTS to PAYROLL.  
`chxgrp Sales parent(PAYROLL) owner(PAYROLL)`
- The user Admin1 wants to change the parent of group projectB from divisionA to divisionB and assign the group RESEARCH as the new owner.  
Admin1 has the ADMIN attribute.

```
chxgrp projectB parent (divisionB) owner (RESEARCH)
```

- The admin user Sally wants to remove the home directory and the shell program specifications for the group profile NewEmployee.  
Sally is the owner of NewEmployee.

```
editgrp NewEmployee homedir() shellprog()
```

- The user Admin1 wants to add the group ProjectA as a child group of the group RESEARCH. The user Admin1 is to be the owner of the ProjectA group.  
Admin1 has the ADMIN attribute.  
The default is owner(Admin1).

```
newgrp ProjectA parent (RESEARCH)
```

## chres Command Modify Resource Records

### Valid in the AC environment

Use the chres, editres, and newres commands to work with resource records that belong to a Privileged Access Manager class. These commands are identical in structure and only vary in the following way:

- The chres command *modifies* one or more resources.
- The editres command *creates or modifies* one or more resources.
- The newres command *creates* one or more resources.

#### NOTE

This command also exists in the native Windows environment but operates differently there.

To add a resource using the newres command, at least one of the following conditions must be true:

- You have the ADMIN attribute.
- You have CREATE access authority in the ACL of the record of the resource class in the ADMIN class.
- If the token use\_unix\_file\_owner in the seos.ini file is set to yes, an owner of a file in UNIX can define it as a new resource to Privileged Access Manager.

To add or change a resource using the chres or editres commands, you must have sufficient authority over the resource. Privileged Access Manager checks in the following order for any *one* of these conditions:

1. You have the ADMIN attribute.
2. The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
3. You are the owner of the record.
4. You are assigned MODIFY (for chres) or CREATE (for editres) access authority in the access control list of the resource class's record in the ADMIN class.

#### NOTE

The maximum length of a resource name is 255 single-byte characters.

The following content lists command parameters that apply for each class that can be administered using the chres, editres, and newres commands.

### ACVAR supported properties

- comment
- owner
- other: VARIABLE\_ TYPE, VARIABLE\_ VALUE

### ADMIN Supported Properties:

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**CALENDAR supported property:**

- comment

**CATEGORY supported property:**

- comment

**CONNECT Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**CONTAINER Supported Properties:**

- audit
- calendar
- comment
- owner
- warning
- other: MEM

**DOMAIN Supported Properties:**



- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**FILE Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- other: MEM

**GFILE Supported Properties:**

- audit
- calendar
- comment
- notify
- owner
- warning
- other: MEM

**GHOST Supported Properties:**

- audit
- calendar
- comment
- owner
- restrictions[-]
- warning
- other: MEM

**GSUDO Supported Properties:**

- calendar
- comment
- defaccess
- owner
- other: MEM

**GTERMINAL Supported Properties:**

- audit
- calendar
- comment
- defaccess
- owner
- restrictions[-]
- other: MEM

**HNODE Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- other: SUBSCRIBER, POLICY

**HOLIDAY Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- other: DATES

**HOST Supported Properties:**

- audit
- calendar
- comment
- owner
- restrictions[-]
- warning

**HOSTNET Supported Properties:**

- audit
- calendar
- comment
- owner
- warning
- other: MASK, MATCH

**HOSTNP Supported Properties:**

- audit
- calendar
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**LOGINAPPL Supported Properties:**

- audit
- calendar
- comment
- defaccess
- notify
- owner
- restrictions[-]
- warning
- other: LOGINFLAGS, LOGINMETHOD, LOGINPATH, LOGINSEQUENCE

**MFTERMINAL Supported Properties:**

- audit
- calendar
- category
- comment
- label
- level
- notify
- owner
- warning
- other: DAYTIME

**POLICY Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- other: SIGNATURE, RULESET

**PROCESS Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**PROGRAM Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- other: TRUST

**PWPOLICY Supported Properties:**

- comment
- owner

**REGKEY Supported Properties:**

- audit
- calendar
- comment
- defaccess
- notify
- owner
- warning
- Other: DAYTIME

**REGVAL Supported Properties:**

- audit
- calendar
- comment
- defaccess
- notify
- owner
- warning
- Other: DAYTIME

**RULESET Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- Other: SIGNATURE, CMD, UNDOCMD

**SECFILE Supported Properties:**

- defaccess
- owner
- Other: TRUST, FLAGS

**SECLABEL Supported Properties:**

- category
- comment
- level
- owner

**SEOS Supported Properties:**

- calendar
- category
- comment
- label
- level
- Other: HOST

**SPECIALPGM Supported Properties:**

- comment
- owner

**SUDO**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning
- Other: TARGUID, PASSWORD

**SURROGATE Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**TCP Supported Properties:**

- audit
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**TERMINAL Supported Properties:**

- audit
- calendar
- category
- comment
- defaccess
- label
- level
- notify
- owner
- restrictions[-]
- warning

**UACC Supported Properties:**

- audit
- category
- comment
- defaccess
- owner

**USER-ATTR Supported Properties:**

- owner
- warning

**USER-DIR Supported Properties:**

- **audit**
- **comment**
- **owner**

```
{{chres|cr}}{{editres|er}}{{newres|nr}} classNameresourceName \
[audit({none|all|success|failure})] \[calendar[-] (calendarName)] \[category[-] (categoryName)]
\[cmd+(selang_command_string) |cmd-] \[comment(string) |comment-] \[container[-] (containerName)]
\[dates(time-period)] \[dh_dr{-|+} (dh_dr)] \[disable|disable-] \[defaccess(accessAuthority)]
\[filepath(filePaths)] \[flags[-|+] (flagName)] \[gacc(access-value)] \[gowner(groupName)] \[host(host-
name) |host-] \[label(labelName) |label-] \[level(number) |level-] \[mask/inetAddress) |match/inetAddress)]
\[mem(resourceName) |mem- (resourceName)] \[node_alias{-|+} (alias)] \[node_ip{-|+} (ip)] \[notify(mailAddress) |
notify-] \[of_class(className)] \[owner({userName | groupName})] \[password | password-]]
\[policy(name(policy-name) {{deviation+|dev+}}|{{deviation-|dev-}})] \[policy(name(policy-name) status(policy-
status) {updater|updated_by}(user-name)) \[{{restrictions}([days({anyday|weekdays|{mon} [tue] [wed] \[thu]
[fri] [sat] [sun]})}]] \[time({anytime|startTime:endTime}) \[restrictions-] \[targuid(userName)] \[trust |
trust-] \[value{+|-} (value)] \[warning | warning-]
```

- **audit**  
Indicates which access events Privileged Access Manager logs:
  - **all** - Both authorized and unauthorized access attempts.
  - **failure** - Unauthorized access attempts. This value is the default.
  - **none** - Does not write any records in the log file.
  - **success** - Authorized access attempts.
- **category(categoryName [,categoryName...])**  
Assigns one or more security categories to the resource record.  
If you specify the category parameter when the CATEGORY class is not active, Privileged Access Manager updates the resource definition in the database. However, the updated category assignment has no effect until the CATEGORY class is activated again.
- **category-(categoryName [,categoryName...])**  
Deletes one or more security categories from the resource record.  
The specified security categories are deleted from the resource record, regardless of whether the CATEGORY class is active. Use this parameter only with the chres or editres command.
- **className**  
Specifies the name of the class to which the resource belongs. To list the resource classes that are defined to Privileged Access Manager, use the find command.
- **cmd+(selang\_command\_string)**  
Specifies a list of selang commands that define the policy. These commands are used to deploy the policy. For example,  

```
editres RULESET IIS5#02 cmd+("nr FILE /inetpub/* defaccess(none) owner(nobody)")
```
- **cmd-**  
Removes policy deployment command list from the RULESET object.
- **comment(string)**  
Adds an alphanumeric string of up to 255 characters to the resource record. If the string contains any blanks, enclose the entire string in single quotation marks. The string replaces any existing string defined previously.

**NOTE**

For the SUDO class, this string has a special meaning. For more information about defining SUDO records, see the *Endpoint Administration Guide for UNIX*.

- **comment-**  
Deletes the comment from the resource record. Use this parameter only with the chres or editres command.
- **container(containerName)**



Represents CONTAINER objects, a generic grouping class.

*containerName* is the name of one or more CONTAINER records defined in the CONTAINER class. When assigning more than one CONTAINER, separate the names with a space or a comma.

- **container-(containerName)**  
Deletes one or more CONTAINER records from the resource record. Use this parameter with the `chres` or `editres` command only.
- **dates(time-period)**  
Defines one or more periods when users cannot log in, such as holidays. If more than one time period is specified, separate the periods with a space. Use the following format:  
`mm/dd[/yy[yy]] [@hh:mm] [-mm/dd]/[/yy[yy]] [@hh:mm]`  
If you do not specify a year (or you specify a year before 1990), it means that the period or holiday is annual. You can specify the year with two digits or four digits. Example: 98 or 1998.  
If you do not specify a start time, then the start of the day (midnight) is used; if you do not specify an end time then the end of the day (midnight) is used. The format of the hours and the minutes is *hh:mm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59).  
If you do not specify an interval of time (for example, 12/25@14:00-12/25@17:00), but only a day and a month (12/25), then the holiday lasts for one whole day.  
If you are issuing the command in a different time zone from where the holiday occurs, translate the period to your local time. For example, if you are in New York and Los Angeles has a half-day holiday, you must enter 09/14/98@18:00-09/14/98@20:00. This prevents the users from logging in from 3:00 pm to 5:00 pm in Los Angeles.
- **defaccess([accessAuthority])**  
Defines the default access authority for the resource. The default access authority is the authority that is granted to any accessor not in the access control list of the resource that requests access to the resource. The default access is also applied to users who are not defined in the database. Valid access authority values vary by class.  
If you omit *accessAuthority*, Privileged Access Manager assigns the implicit access that is specified in the UACC property of the record that represents the class of the resource in the UACC.
- **dh\_dr{+|-}(dh\_dr)**  
Defines Distribution Hosts this endpoint uses for disaster recovery.
- **filepath(filePaths)**  
Defines one or more absolute file paths, each of which constitutes a valid kernel module. Multiple file paths are separated by a colon (:).
- **flags(flagName)**  
Defines how the resource is to be trusted and how to check it for trusted status. Available flags are Ctime, Mtime, Mode, Size, Device, Inode, Crc, and Own/All/None.
- **gacc(access-value)**  
Lets a program access protected, frequently opened files at a much faster rate than otherwise possible.
- **gowner(groupName)**  
Assigns a Privileged Access Manager group as the owner of the resource record. The group owner of the resource record has unrestricted access to the resource, as long as the following criteria are true: the security level of the group owner, security label, and security category authorities are sufficient to allow access to the resource. The group owner of the resource is always permitted to update and delete the resource record. See the *Endpoint Administration Guide for UNIX* for more information.
- **label(labelName)**  
Assigns a security label to the resource record.
- **label-**  
Deletes the security label from the resource record. Use this parameter only with the `chres` or `editres` command.
- **level(number)**  
Assigns a security level to the resource record. Enter a positive integer from 1 through 255.
- **level-**  
Removes any security level from the resource. Use this parameter only with the `chres` or `editres` command.
- **mask (IPv4-address)** and **match (IPv4-address)**

The *mask* and *match* parameters are applicable only to HOSTNET records. They are required when creating a HOSTNET record and are optional when modifying a record.

Use mask and match together to define the group of hosts defined by a HOSTNET record. A host is a member of a HOSTNET record group if an AND of the host IP address with the mask address produces the match address. For example, specifying mask(255.255.255.0) and match(192.16.133.0) means that a host is a member of the group if it has an IP address in the range 192.16.133.0 to 192.16.133.255.

The mask and match parameters require IPv4 addresses.

- **mem(resourceName)**

Adds a member resource to a resource group. If you are adding more than one member resource, separate each name with a comma.

You can use the mem parameter only with resource records of the following classes:

- CONTAINER - This class defines a group of objects from other resource classes.
- GFILE - This class contains resource records that define groups of files.
- GHOST - This class contains resource records that define groups of hosts.
- GSUDO - This class contains resource records that define groups of commands.
- GTERMINAL - This class contains resource records that define groups of terminals.
- GPOLICY - This class contains resource records that define a logical policy.
- GHNODE - This class contains resource records that define a host group.
- GDEPLOYMENT - This class contains resource records that define the policy deployment.

Use the mem parameter to add a record of the appropriate type to a resource group, for example, to add a FILE record to a resource group of class GFILE.

**NOTE**

If you are using the mem parameter for CONTAINER resources, you must also include the of\_class parameter.

Both the member resource and the resource group must already be defined in Privileged Access Manager. To create a resource group, create a resource of the class you want. For example, the following command creates a GFILE resource group:

```
newres GFILE myfiles
```

- **mem-(resourceName)**

Removes member resources from a resource group. If you are removing more than one member resource, separate the resource names with a space or a comma. Use this parameter only with the chres or editres command.

- **node\_alias{-|+}(alias)**

Defines an endpoint alias.

Defining aliases for the endpoint aliases lets Privileged Access Manager send advanced policy management commands to the actual endpoint based on the alias.

- **node\_ip{-|+}(ip)**

Defines the IP address of the host. Advanced policy management uses the IP address, with the name of the endpoint, to locate the required endpoint.

- **notify(mailAddress)**

**NOTE**

Instructs Privileged Access Manager to send notification messages whenever the resource that is represented by the resource record is accessed. Enter a user name, an email address of a user, or the email address of a mail group if an alias is specified.

Notification takes place only when the Log Routing System is active. The notification messages are sent either to the screen or to the mailbox of the users, depending on the setup of the Log Routing System.

Each time a notification message is sent, an audit record is written in the audit log. For information about filtering and viewing audit records, see the *Endpoint Administration Guide for UNIX*.

The recipient of notify messages should log in frequently to respond to the unauthorized access attempts described in each message.

**Limit:** 30 characters.

- **notify-**  
Specifies that no one is notified when the resource that is represented by the resource record is successfully accessed. Use this parameter only with the `chres` or `editres` command.
- **of\_class(className)**  
Specifies the resource type for the record you are adding to the CONTAINER class with the `mem` parameter.
- **owner(Name)**  
Assigns a Privileged Access Manager user or group as the owner of the resource record. The owner of the resource record has unrestricted access to the resource, provided the security level of the owner, security label, and security category authorities are sufficient to allow access to the resource. The owner of the resource is always permitted to update and delete the resource record. See the *Endpoint Administration Guide for UNIX* for more information.
- **password**  
Specifies, for the SUDO class, that the `sesudo` command requires the original password of the user.
- **password-**  
Cancels the `password` parameter, so that the `sesudo` command no longer requires the original password of the user. Use this parameter with the `chres` or `editres` command only. If the `password` parameter was not used previously, then this parameter is unnecessary.
- **policy(name(name#xx) status(status) updated\_by(name)) | policy(name(name#xx) deviation{+|-})**  
Adds a subscriber of the node in the propagation tree and specifies its status. Alternatively, updates an existing policy version to specify whether a policy deviation exists or not. The `updated_by` property must be updated when updating policy status. It is a string representing the name of the user that changed the policy status.  
Policy status can be one of Transferred, Deployed, Undeployed, Failed, SigFailed, Queued, UndeployFailed, or TransferFailed.
- **policy-[(name(name#xx))]**  
Removes the named policy version from the node. If no policy is specified, all policies that are deployed to this node are removed.
- **resourceName**  
Defines the name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses. Separate the resource names with a space or a comma. At least one resource name must be specified.  
Privileged Access Manager processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.  
**Note:** If you use a variable in a resource name, use the following syntax to refer to the variable: `<!variable>`, for example, `<!AC_ROOT_PATH>\bin`. You can only use variables in `selang` rules in policies.
- **restrictions([days] [time])**  
Specifies the days of the week and the hours in the day when users can access the file.  
If you omit the `days` argument and specify the `time` argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit `time` and specify `days`, the day restriction applies to any time restriction already indicated in the record. If you specify both `days` and `time`, the users may access the system only during the specified time period on the specified days.
  - [Days] specifies the days on which users may access the file. The `days` argument takes the following subarguments:
    - a. **anyday**-Allow users access to the file on any day.
    - b. **weekdays**-Allow users access to the resource only on weekdays-Monday through Friday.
    - c. **Mon, Tue, Wed, Thu, Fri, Sat, Sun**-Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
  - [Time] specifies the period during which users may access the resource. The `time` argument takes the following subarguments:
    - a. **anytime**-Allow users access to the resource at any time of the day.

- b. **startTime:endTime**-Allow access to the resource only during the specified period. The format of both **startTime** and **endTime** is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. **startTime** must be less than **endTime**, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 am to 5:00 pm in Los Angeles, specify time (1100:2000).
  - **restrictions-([days] [time])**  
Deletes any restrictions that limit the ability of the user to access the file.
  - **ruleset+(name)**  
Specifies a rule set to associate with the policy.
  - **ruleset-(name)**  
Deletes a rule set from the policy. If no ruleset is specified, removes all rulesets from the policy.
  - **signature(hash\_value)**  
Specifies a hash value. For a policy, this is based on signatures of RULESET objects associated with the policy. For a ruleset, this is based on the policy deployment command list and policy undeployment (removal) command list.
  - **subscriber(name(sub\_name) status(status))**  
Adds a subscriber of the node in the propagation tree and specifies its status. Status can be one of **unknown**, **available**, **unavailable**, or **sync**.
  - **subscriber-(name(sub\_name)) | sub-**  
Removes a subscriber database from the node. If no subscriber is specified, all subscribers are removed.
  - **targuid(userName)**  
Specifies, for the SUDO class, the name of the user whose authority is borrowed for executing the command. Default is root.
  - **trust**  
Specifies that the resource is trusted. The trust parameter applies only to resources of the PROGRAM and SECFILE classes. Users can execute the program as long as the program remains trusted. See the *Endpoint Administration Guide for UNIX* for more information. Use this parameter only with the **chres** or **editres** command.
  - **trust-**  
Specifies that the resource is untrusted. The trust- parameter applies only to resources of the PROGRAM and SECFILE classes. Users cannot execute an untrusted program. See the *Endpoint Administration Guide for UNIX* for more information. Use this parameter only with the **chres** or **editres** command.
  - **undocmd+(selang\_command\_string)**  
Specifies a list of selang commands that define policy undeployment. The commands in this list are used to remove the deployed policy (undeploy). For example:  

```
editres RULESET IIS5#02 undocmd+("rr FILE /inetpub/*")
```
  - **undocmd-**  
Removes policy removal command list from the RULESET object.
  - **value+(value)**  
Adds the specified value to the specified variable (ACVAR object).
  - **value-(value)**  
Removes the specified value from the specified variable (ACVAR object).
  - **warning**  
Specifies that Privileged Access Manager allows access to the resource even if the authority of the accessor is insufficient to access the resource. However, Privileged Access Manager writes a warning message in the audit log.
- NOTE**  
In Warning Mode, Privileged Access Manager does not create warning messages for the resource groups.
- **warning-**

Specifies that Privileged Access Manager is to deny the user access to the resource. Does not write a warning message if the authority of an accessor is insufficient to access the resource. Use this parameter only with the `chres` or `editres` command.

## Examples

- The user (`admin1`) wants to change the owner and default access for the terminal (`tty30`) and restrict the use of the terminal to weekdays during regular business hours (8:00 am to 6:00 pm).
  - The user `admin1` has the `ADMIN` attribute.

```
chres TERMINAL tty30 owner(admin1) defaccess(read) restrictions \(days(weekdays)time(0800:1800))
```
- The admin user Sally wants to remove the group and owner property stored in a `FILE` class record for file `account.txt`.
  - The user Sally is the owner of the user record of Jared.

```
chres FILE /account.txt group() owner()
```

To remove any record property, if a string defines the property, type the property with either the `-` sign or empty parenthesis `()`.
- The user Bob wants to delete the comment field of the terminal `tty190` and be notified whenever access to the terminal is granted.
  - The user Bob is a Privileged Access Manager user and is the owner of the terminal `tty190`.

```
chres TERMINAL tty190 comment- notify(Bob@athena)
```
- The user `Admin1` wants to add the `OPERATOR` category to the list of security categories of the resource `USER.root`, which is in the `SURROGATE` class.
  - The user `Admin1` has the `ADMIN` attribute.
  - The `OPERATOR` category is defined in the database.

```
chres SURROGATE USER.root category(OPERATOR)
```
- The user `admin1` wants to define `/bin/su` as a trusted program with a global access of `EXECUTE`.
  - The user `admin1` has the `ADMIN` attribute.
  - The following defaults apply:
    - `restrictions(days(anyday) time(anytime))`
    - `owner(admin1)`
    - `audit(failure)`

```
newres PROGRAM /bin/su defaccess(x) trust
```
- The user `admin1` wants to define the substitution of group ID to the group system as a protected resource to which no user, including `admin1`, has access.
  - The user `admin1` has the `ADMIN` attribute. The user `nobody` is defined to Privileged Access Manager.
  - The following defaults apply:
    - `restrictions(days(anyday) time(anytime))`
    - `audit(failure)`

```
newres SURROGATE GROUP.system defaccess(n) owner(nobody)
```
- The user `SecAdmin` wants to define `ProjATerms`, a group of terminals containing the terminals `T1`, `T8`, and `T11`. The terminal group is to be used only by the group `PROJECTA` and only on weekdays during regular business hours (8:00 am to 6:00 pm).
  - The user `SecAdmin` has the `ADMIN` attribute.
  - The terminals `T1`, `T8`, and `T11` are defined to Privileged Access Manager.
  - The group `PROJECTA` is defined to Privileged Access Manager.
  - `audit(failure)`

```
newres GTERMINAL ProjATerms mem(T1,T8,T11) owner(PROJECTA) \restrictions(days(weekdays) time(0800:1800))
defaccess(n)
```

## ch x usr Command Change User Properties

### Valid in the AC environment

Use the commands `chusr`, `chxusr`, `editusr`, `editxusr`, `newusr`, and `newxusr` to change the properties of users, and to define the user records in the Privileged Access Manager database if necessary.

These commands all have synonyms, as follows:

- `chusrcu`
- `chxusrcxu`
- `editusreu`
- `editxusrexu`
- `newusrnu`
- `newxusrnxu`

This means, for example, that the command `cu` is identical to the command `chusr`.

All these commands are identical in structure, and vary only in their scope. Use these commands as follows:

- Use the `chusr`, `editusr`, and `newusr` commands for internal users. The differences between these commands are as follows:
  - The `chusr` command *modifies* one or more USER records.
  - The `editusr` command *creates or modifies* one or more USER records.
  - The `newusr` command *creates* one or more USER records.

#### NOTE

These commands also exist in the native environment but operate differently there.

- Use the `chxusr`, `editxusr` and `newxusr` commands for enterprise users. The differences between these commands are as follows:
  - The `chxusr` command *modifies* one or more XUSER records.
  - The `editxusr` command *creates or modifies* one or more XUSER records.
  - The `newxusr` command *creates* one or more XUSER records.

#### NOTE

The USER and XUSER class records are identical for all properties, except that where properties are defined in the enterprise user stores, the XUSER records do not redefine them.

#### NOTE

When you execute these commands, the changes that you make modify the user record immediately, even if the user is currently logged in to the system.

### Authorization Required

To create a Privileged Access Manager user, at least one of the following conditions must be true:

- You have the ADMIN attribute.
- You are assigned the CREATE authority in the access control list of the USER or XUSER record in the ADMIN class.

To add or modify a user, at least one of the following conditions must be true:

- You have the ADMIN attribute.
- The user record is within the scope of a group in which you have the GROUP-ADMIN attribute and you have the same authority as the owner of the record.
- The user record is within the scope of a group in which you have the GROUP-AUDITOR attribute, and you want to specify the audit parameter.
- You are the owner of the group.
- You are assigned the MODIFY (for ch[x]usr) or CREATE (for edit[x]usr) authority in the access control list of the USER or XUSER record in the ADMIN class.

```
{ {chusr|cu} | {chxusr|cxu} | {editusr|eu} | {editxusr|exu} | {newusr|nu} | {newxusr|nxu} } \
{userName | (userName [,userName...])} \
[{admin | admin-}] \
[audit({none | all | {{success}[failure][loginsuccess][loginfail][trace][interactive]}})] \
[{auditor | auditor-}] \
[{category(categoryName) | category-(categoryName)}] \
[{comment(string) | comment-}] \
[country(string)] \
[email(emailAddress)] \
[enable] \
epwasown(password) \
[{expire[(date)] | expire-}] \
[fullname (fullName)]
[owner(groupName)] \
[{grace(nLogins) | grace-}] \
[{ign_hol | ign_hol-}] \
[{inactive(nDays) | inactive-}] \
[{interval(nDays) | interval-}] \
[{label(labelName) | label-}] \
[{level(number) | level-}] \
[location(string)] \
[{logical|logical-}] \
[{maxlogins(nLogins) | maxlogins-}] \
[{min_life(nDays) | min_life-}] \
[{notify(mailAddress) | notify-}] \
[{operator | operator-}] \
[organization(string)] \
[org_unit(string)] \
[owner({userName | groupName})] \
[password(string)] \
[phone(string)] \
[{pmdb(pmdbName) | pmdb-}] \
[{profile(groupName) | profile-}] \
[pwasown(string)] \
[{pwmanager | pwmanager-}] \
[regular] \
[{restrictions( \[days({anyday|weekdays[mon] [tue] [wed] [thu] [fri] [sat] [sun])}] \[time({anytime|
startTime:endTime})] | restrictions-}] \
[{resume[(date)] | resume-}] \
[{server | server-}] \
[{suspend[(date)] | suspend-}] \
[nt|nt ( \[admin|admin-] \[comment('comment')|comment- \[country('country-name')] \[expire|expire(mm/
dd/yy[@hh:mm])|expire-] \[flags({account-flags}|account-flags)] \[homedir(any-string)] \[homedrive(home-
drive)] \[location(any-string)] \[logonserver(server-name)] \[name(full_name)] \[organization(name)]
```



```

\[org_unit(name)] \[password(user's temporary password)] \[pgroup(primary-group)] \[phone(any-string)]
\[privileges(privilege-list)] \[restrictions(days(day-data) time(hhmm:hhmm|anytime) )] \[script(logon-script-
path)] \[workstations(workstations-list)] ]] \
[unix({ [gecos(string)] \[homedir(path)] \[pgroup(groupName)] \[shellprog(fileName)] \[userid(number)]}]

```

- **admin**  
Assigns the ADMIN attribute to the user. A user with the ADMIN attribute is allowed to issue all selang commands with all parameters except the audit parameter. You must have the ADMIN attribute to use the admin parameter.
- **admin-**  
Removes the ADMIN attribute from the user. (Privileged Access Manager verifies that at least one user has the ADMIN attribute.)  
You cannot use this parameter with the new[x]usr command.
- **audit**  
Specifies which user activities on resources protected by Privileged Access Manager are logged to the audit log. To specify more than one event type, separate the event type names with a space or a comma. Privileged Access Manager logs activities based on these attributes:
  - **all** - All user activities. The monitored activities are: failure, loginfail, loginsuccess, success, interactive and trace.
  - **failure** - Failed access attempts.
  - **loginfail** - Failed login attempts.
  - **loginsuccess** - Successful logins.
  - **none** - No user activities.
  - **success** - Successful accesses.
  - **interactive** - Interactive sessions.
  - **trace** - Every message that appears in the trace file because of this user's actions.
- **auditor**  
Assigns the AUDITOR attribute to the user. A user with the AUDITOR attribute can audit the use of system resources and is able to control the logging of detected accesses to any Privileged Access Manager-protected resource during Privileged Access Manager authorization checking and accesses to the database. See the *Endpoint Administration Guide* for your OS for more information about the authorities granted to a user with the AUDITOR attribute.
- **auditor-**  
Removes the AUDITOR attribute from the user record.  
You cannot use this parameter with the new[x]usr command.
- **auth\_type**  
Specifies the authentication method.  
Used only by SSO.  
You cannot use this parameter for enterprise users.
- **category(categoryName[, categoryName...])**  
Assigns one or more security categories to the user.
- **category-(categoryName[, categoryName...])**  
Removes one or more security categories from the user record.  
You cannot use this parameter with the new[x]usr command.
- **comment(commentString )**  
Assigns a comment to the user record.
  - *commentString*  
Specifies the comment. *commentString* is an alphanumeric string of up to 255 characters. If *commentString* contains blanks, enclose it in single quotation marks.
- **comment-**  
Deletes the comment from the user record.  
You cannot use this parameter with the new[x]usr command.
- **country(countryName)**



Specifies the country where the user is located. The country is not used during the authorization process.

- *countryName*  
Defines the country. This parameter is an alphanumeric string of up to 19 characters. If the string contains blanks, enclose the entire string in single quotation marks.
- *email(emailAddress)*  
Defines the email address of the user.
  - *emailAddress*  
Defines the email address of the user.  
**Limits:** Up to 128 characters
- **enable**  
Enables the login of a user that has for any reason been disabled.  
You cannot use this parameter with the `new[x]usr` command.
- *epwasown(password)*  
Changes the user password as if the user changes their own password. This password change is not an administrative change and so does not automatically expire the password.  
**Note:** This command is for internal use only. This command sets password in plain text as specified as an argument to `/etc/shadow` or the `passwd` file.
- *expire(dateTime)*  
Sets the date when the user account expires. If a date is not specified, the account expires immediately, or if the user is logged in, when the user logs out.  
If the user record has a value for this property, that value overrides the value in the GROUP record.

#### NOTE

Use the `expire-` parameter to enable expired user records; you do not use the `resume` parameter to do this.

- *dateTime*  
Defines the date, and optionally the time. It has the following format: `mm/dd/[yy]yy[ @HH:MM]`  
You can use either two digits or four digits to specify the year.
- **expire-**  
For the `new[x]usr` command, defines a user account that does not have an expiration date.  
For the `ch[x]usr` and `edit[x]usr` commands, removes an expiration date from a user account.
- *flags(accountFlags|-accountFlags)*  
Specifies particular attributes of a user's account. See the appendix Windows Values for a list of valid flag values.  
To remove flags from the user record, precede *accountFlags* with a minus (-).
- *fullName(fullName)*  
Specifies the full name of the user.
  - *fullName*  
Defines the full name. It is an alphanumeric string of up to 255 characters. If *fullName* contains blanks, enclose the entire string in single quotation marks.
- *gecos(string)*  
Specifies a comment string for the user. Enclose the string in single quotation marks.
- *gowner(groupName)*  
Assigns a Privileged Access Manager group as the owner of the user record. The group owner of the user record has unrestricted access to it, provided the group owner's security level and security category authorities are sufficient. The group owner of the user record is always permitted to update and delete the user record.
- *grace(nLogins)*  
Defines the number of grace logins the user is allowed.  
After the number of grace logins is reached, the user cannot access the system and must contact the system administrator to select a new password. If `grace` is set to zero, the user cannot log in.  
If the user record has a value for this parameter, that value overrides the value in the GROUP record.

If this parameter is not specified and the user has a profile group that contains a value for this parameter, the value in the GROUP record is used. If neither the USER nor GROUP record contains a value, the Privileged Access Manager global grace login setting is used.

– *nLogins*

Defines the number of grace logins. Enter an integer between 0 and 255.

**NOTE**

The user should change the password before the grace value reaches 0. Contact the system administrator to select a new password if the grace login value is reached.

- **grace-**

Deletes the user's grace login setting. The Privileged Access Manager global grace login setting is used instead. You cannot use this parameter with the `newusr` command.

- **homedir(*path*)**

Specifies the full path of the user's home directory. If *path* ends with a slash, Privileged Access Manager concatenates *userName* to the path.

- **homedrive(*drive*)**

Specifies the drive of the user's home directory.

- **ign\_hol**

Assigns the IGN\_HOL attribute to the user. A user with the IGN\_HOL attribute can log in during any period defined in a holiday record.

- **ign\_hol-**

Removes IGN\_HOL attribute from the user.

- **inactive(*nDays*)**

Specifies the number of days that must pass before the system changes the user to inactive. When the number of days is reached, the user cannot log in.

**NOTE**

Inactive users are not marked in the user record. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

– *nDays*

Defines the number of days. *nDays* is zero or a positive integer. If *nDays* is zero, the effect is the same as using the `inactive-` parameter.

- **inactive-**

Changes the user's status from inactive to active. You cannot use this parameter with the `newusr` command.

- **interval(*nDays*)**

Defines the number of days that must pass after the password was set or changed before the system prompts the user for a new password. Enter zero or a positive integer. If *nDays* is zero Privileged Access Manager disables password interval checking and the password does not expire. This means the default set by the `setoptions` command is not used. Set *nDays* to zero only for users with low security requirements.

When *nDays* is reached, Privileged Access Manager informs the user that the password has expired. The user can continue to use the password until the number of grace logins is reached. After the number of grace logins is reached, the user is denied access to the system and must contact the system administrator to be given a new password.

- **interval-**

Cancels a user's password interval setting. If the user has a profile group with a value for this parameter, that value is used. Otherwise, the default set by the `setoptions` command is used. You cannot use this parameter with the `new[x]usr` command.

- **label(*labelName*)**

Assigns a security label to the user.

- **label-**

Deletes the security label from the user record.

You cannot use this parameter with the `new[x]usr` command.

- **level(*levelNumber*)**  
Assigns a security level to the user record.  
*levelNumber* is an integer between 0 and 255.
- **level-**  
Deletes the security level from the user record,  
You cannot use this parameter with the `newusr` command.
- **localapps**  
Used by CA SSO.
- **location(*locationString*)**  
Specifies the user's location. The location is not used during the authorization process.
  - *locationString*  
Defines the location. *locationString* is an alphanumeric string of up to 47 characters. If *locationString* contains blanks, enclose it in single quotation marks.
- **logical**  
Assigns the LOGICAL attribute to the user. A user with the LOGICAL attribute cannot log in and is used for internal Privileged Access Manager purposes only.  
For example, the user `nobody` that you can use as the owner of resources to prevent even the resource owner from accessing the resource is a logical user by default. This means that no user can log in using this account.
- **logical-**  
Removes the LOGICAL attribute from the user.
- **logonserver(*server-name*)**  
Specifies the server that verifies the login information for the user. When the user logs in to the domain workstation, Privileged Access Manager transfers the login information to the server, which gives the workstation permission for the user to work.
- **maxlogins(*nLogins*)**  
Sets the maximum number of concurrent logins for the user. A value of 0 (zero) means that the user can log in from any number of terminals concurrently. If this parameter is not specified, the global maximum logins setting is used.

#### NOTE

If `maxlogins` is set to 1, you cannot run `selang`. You must shut down Privileged Access Manager, change the `maxlogins` setting to greater than one, for example by using `setpropadm` utility, and start Privileged Access Manager again.

- **maxlogins-**  
Deletes the user's maximum login setting. The global setting is used instead.  
You cannot use this parameter with the `new[x]usr` command.
- **min\_life(*nDays*)**  
The minimum number of days that must pass before the user is allowed to change the password again. Enter a positive integer.
- **min\_life-**  
Deletes the user's `min_life` setting. If the user has a profile group with a value for this parameter, that value is used. Otherwise, the default set by the `setoptions` command is used.  
You cannot use this parameter with the `new[x]usr` command.
- **nochngpass**  
Specifies that the user is not allowed to change passwords for another user.
- **notify(*notifyAddress*)**  
Sends an email to *notifyAddress* every time the user logs in. The recipient of the notify messages should log in frequently to respond to the unauthorized access attempts described in each message.  
When Privileged Access Manager sends a notification message, it writes an audit record in the audit log.
  - *notifyAddress*  
Defines a user name or an email address.

**Limit:** 30 characters.

- **notify-**  
Specifies that no one is notified when the user logs in.  
You cannot use this parameter with the new[x]usr command.
- **nt**  
For the chusr and editusr commands, this parameter changes the user's definition in the local Windows system.  
For the newusr command, this parameter adds the user to the local Windows system.  
If more than one argument is specified, separate the arguments with a space.  
See the environment command, for more information about how to operate on the local Windows system from within Privileged Access Manager.  
The nt option, and sub-options under the nt option, are not valid for enterprise users.
- **operator**  
Assigns the OPERATOR attribute to the user. A user with the OPERATOR attribute can list all resource records in the database, and has read authority for all Privileged Access Manager defined files.  
A user with this attribute can also use all the options of the secons command. See the *Reference Guide* for more information about the secons utility.
- **operator-**  
Removes the OPERATOR attribute from a user record.  
You cannot use this parameter with the newusr command.
- **organization(*organizationString*)**  
Specifies the user's organization. The organization is not used during the authorization process.
  - *organizationString*  
Defines the organization. *organizationString* is an alphanumeric string of up to 255 characters. If *organizationString* contains blanks, enclose it in single quotation marks.
- **org\_unit(*org\_unitString*)**  
Specifies the user's organization unit. The organization unit is not used during the authorization process.
  - *org\_unitString*  
Defines the organization unit. *org\_unitString* is an alphanumeric string of up to 255 characters. If *organizationString* contains blanks, enclose it in single quotation marks.
- **owner(*Name*)**  
Assigns a Privileged Access Manager user or group as the owner of the user record. See the *Endpoint Administration Guide* for your OS for more information.
- **password(*string*)**  
Assigns a password to a user. Specify any character except a space or a comma. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, a new password must be set.  
To change your own password, you need to set selang options using *setoptions cng\_ownpwd* or use sepass.
- **pgroup(*groupName*)**  
Sets the user's primary group ID. *groupName* is the name of a UNIX group.
- **phone(*phoneString*)**  
Defines the user's telephone number. The telephone number is not used during the authorization process.
  - *phoneString*  
Defines the telephone number. *phoneString* is an alphanumeric string of up to 19 characters. If *phoneString* contains blanks, enclose it in single quotation marks.
- **pmdb(*pmdbName*)**  
Specifies that when a user changes a password with the sepass utility, the new password is propagated to the specified PMDB. Enter the fully qualified name of the PMDB. The password is not sent to the Policy Model defined in the parent\_pmd or passwd\_pmd tokens in the [seos] section of seos.ini.  
This option cannot be used for enterprise users.
- **pmdb-**  
Removes the PMDB attribute from the user record.

You cannot use this parameter with the new[x]usr command.

- **privileges(*privilege-list*)**  
Adds specific rights to the Windows user record or, when privList is preceded by a minus sign (-), removes the specified rights.  
You cannot use this parameter with the newusr command.
- **profile(*groupName*)**  
Assigns a user to a profile group. The following values can be taken from the profile group:
  - audit
  - auth\_type
  - expire
  - grace
  - inactive
  - interval
  - maxlogins
  - min\_life
  - password rules
  - pmdb
  - pwd\_autogen
  - pwd\_policy
  - pwd\_sync
  - restrictions (days, time)
  - resume
  - suspend
  - unix (homedir, shellprog)
- **profile-**  
Removes a user from the profile group.  
You cannot use this parameter with the new[x]usr command.
- **pwmanager**  
Assigns the PWMANAGER attribute to the user. A user with this attribute can change the passwords of users in the database. See the *Endpoint Administration Guide* for your OS for more information.
- **pwmanager-**  
Removes the PWMANAGER attribute from the user record.  
You cannot use this parameter with the new[x]usr command.
- **pwasown(*string*)**  
Replaces a password as if changed by the user. Specifying this parameter updates the time and date of the last change in the database. Grace logins are terminated.
- **regular**  
Resets the OBJ\_TYPE property of the record, and so removes authority attributes from the user.
- **restrictions([*Days*] [*Time*])**  
Specifies the days of the week and the times in the day when users can be logged in. The restrictions are stored in the DAYTIME property of the [X]USER record.  
If you omit *Days* and specify *Time*, the time restriction applies to any day-of-week restriction that is already defined in the record.  
If you omit *Time* and specify *Days*, the *Days* restriction applies to any time restriction already defined in the record.  
If you specify both *Days* and *Time*, the users can access the system only during the specified time period on the specified days.
  - *Days*  
Specifies the days on which users can be logged in. You can use the following keywords when you specify *Days*:
    - a. **anyday** Allow users access to the file on any day.

- b. **weekdays** Allow users access to the resource only on weekdays-Monday through Friday.
- c. **Mon, Tue, Wed, Thu, Fri, Sat, Sun** Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
- **Time**  
Specifies the period during which users can be logged in. The time argument takes the following sub-arguments:
  - a. **anytime** Allow users access to the resource at any time of the day.
  - b. **startTime : endTime** Allow access to the resource only during the specified period.  
The format of *startTime* and *endTime* is *hhmm*, where *hh* is the hour (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value; use 0000 instead.  
*startTime* must be less than *endTime*.  
**Note:** Privileged Access Manager uses the time zone of the processor. If the user logs in at a terminal in a different time zone from the processor, you must take this into account.
- **restrictions-([days] [time])**  
Deletes any restrictions that limit the users' ability to be logged in.
- **resume([dateTime])**  
Enables a user record that was disabled by specifying the suspend parameter. If you specify both the suspend parameter and the resume parameter, the resume date must fall after the suspend date. If you omit *dateTime*, the user record is resumed immediately upon execution of the *chusr* command. See the *Endpoint Administration Guide* for your OS for more information.  
Enter *dateTime* in the format *[m]m/[d]d/yy[@HH:MM]*.
- **resume-**  
Erases the resume date, and time if used, from the user record. Consequently, the status of the user is changed from active (enabled) to suspended.  
You cannot use this parameter with the *new[x]usr* command.
- **script(logon-script-path)**  
Specifies the location of a file that runs automatically when the user logs in. This parameter is optional. Typically, this login script configures the working environment. You can also use the profile parameter to set up the user's working environment.
- **server**  
Sets the SERVER attribute on. This attribute allows a process running on behalf of the current user to ask for authorization for other users. See the *Endpoint Administration Guide* for your OS for more information.
- **server-**  
Sets the SERVER attribute off.  
You cannot use this parameter with the *new[x]usr* command.
- **shellprog(fileName)**  
Specifies the full path of the initial program or shell that is executed after the user invokes the login or su command.  
*fileName* is a character string.  
This option cannot be used for enterprise users.
- **suspend([dateTime])**  
Disables a user record, but leaves it defined in the database. A user cannot use a disabled user account to log in to the system.  
If *dateTime* is specified, the user record is disabled on the specified date. If *dateTime* is omitted, the user record is disabled immediately upon execution of the *ch[x]usr* command.  
Enter *dateTime* in the format *mm/dd/yy[@HH:MM]*.
- **suspend-**  
Erases the suspend date from the user record, changing the status of the user from disabled to enabled (active).  
You cannot use this parameter with the *new[x]usr* command.
- **unix**  
For the *chusr* and *editusr* commands, this parameter changes the user's definition in the local UNIX system.  
For the *newusr* command, this parameter adds the user to the local UNIX system.  
If more than one argument is specified, separate the arguments with a space.

See the environment command in this chapter for more information about how to operate on the local UNIX system from within Privileged Access Manager.

The unix option, and sub-options under the unix option are not valid for enterprise users.

- **userid(*number*)**  
Sets the user's unique numeric ID (UID), used for unique discretionary access control. *number* is a decimal number. By default, numbers less than 100 are not accepted. See the AllowedGidRange token in the appendix *Reference Guide* for more information about excluded numbers.
- **userName|(userName [,userName...])**  
Defines the name or names of the user or users. Each user name must be unique.  
When using the newusr command, *userName* identifies a new user to Privileged Access Manager. If you are using the newusr command and the user is already defined to the native environment, this username will be used by Privileged Access Manager as the USER record that corresponds to that user. Typically, however, you should take advantage of the Privileged Access Manager ability to use enterprise users, and not use newusr to create a USER record for a username that already exists in the native environment. Instead, use the chgxusr command to change the Privileged Access Manager properties of that user.  
Sometimes you may want a Privileged Access Manager user name that is not a native login name. In that case, the login command could not put that user to work, but another command such as sesu could.

#### NOTE

ON UNIX, where a user name includes a backslash, use two backslashes when specifying *userName*.

#### Examples

- The user Bob wants to add the FINANCIAL category to Jim's record, change Jim's security level to 155, and restrict Jim's access to the system to weekdays between 8:00 a.m. and 8:00 p.m.
  - The user Bob has the ADMIN attribute.
  - The user Jim is defined to Privileged Access Manager.
  - The FINANCIAL category is defined to Privileged Access Manager.

```
chuxsr Jim category(FINANCIAL) level(155) restrictions \
(days(weekdays)time(0800:2000))
```
- The user admin wants to suspend the user Joel, who will be on vacation for three weeks, starting on August 5, 1995.
  - The user admin has the ADMIN attribute.
  - The user Joel is defined to Privileged Access Manager.
  - Today's date is August 3, 1994.

```
chxusr Joel suspend(8/5/95) resume(8/26/95)
```
- The user Security2 wants to remove the AUDITOR attribute from the user Bill and wants to audit all activity by Bill.
  - The user Security2 has the ADMIN and AUDITOR attributes.
  - The user Bill is defined to Privileged Access Manager.

```
chxusr Bill auditor audit(all)
```
- The user Rob wants to change the comment stored in the record of the user Mary.
  - The user Rob is the owner of Mary's user record.

```
chxusr Mary comment ('Administrator of the SALES group')
```
- The admin user Sally wants to remove the country name and the location properties stored in the record of the user Jared.
  - The user Sally is the owner of Jared's user record.

```
chxusr Jared country() location()
```
- The user Bob wants to define the users Peter and Joe to Privileged Access Manager.
  - The user Bob has the ADMIN attribute.
  - The users Peter and Joe are not defined to Privileged Access Manager.
  - The following defaults apply:



- owner(Bob)
- audit(failure,loginfailure)

```
newusr (Peter Joe)
```

- The user Bob wants to define the user Jane to Privileged Access Manager and assign payroll as the owning group.
  - The user Bob has the ADMIN attribute.
  - The user Jane is not defined to Privileged Access Manager.
  - The full name of the user Jane is JG Harris.
  - audit(failure,loginfailure)

```
newusr Jane owner(payroll) name('J.G. Harris')
```

- The user Bob wants to define the user *JohnD* to Privileged Access Manager with the security category NewEmployee and a security level of three. JohnD is to be allowed to use the system only on weekdays between the hours of 8:00 a.m. and 6:00 p.m.
  - The user Bob has the ADMIN attribute.
  - The NewEmployee category is defined to Privileged Access Manager.
  - The new user's full name is John Doe.
  - The following defaults apply:
    - owner(Bob)
    - audit(failure)

```
newusr JohnD name('John Doe') category(NewEmployee) level(3) \
restrictions(days(weekdays) time(0800:1800))
```

## deploy Command Initiate Policy Deployment

### Valid in the AC environment

Use the deploy command to initiate policy deployment. The command executes selang commands stored with the RULESET object that is associated with the POLICY object you are deploying. These are policy deployment commands.

#### **WARNING**

We strongly recommend that you use the policydeploy utility to deploy a stored policy. The deploy command only executes part of the policy deployment and does not update the DMS when deploying a policy to an endpoint.

To run the deploy command, you need to have:

- Sub-administration rights for the POLICY, HNODE, and RULESET classes on each database in the hierarchy below the database where you deploy the policy.
- Appropriate sub-administration rights on each database in the hierarchy below the database where you deploy the policy.

These are the permissions necessary to execute the selang commands that form the policy on each of these computers.

For example, you'll need sub-administration rights for the FILE class if you are creating a new file resource:

```
nr FILE /inetpub/* defaccess(none)
```

#### **NOTE**

For more information about policy deployment, see the *Enterprise Administration Guide*.

This command has the following format:

```
deploy POLICY name#xx
```

- *name#xx*  
The name of the POLICY object (policy name and version number) for the policy you want to deploy.



## deploy- Command Initiate Policy Removal

### Valid in the AC environment

Use the deploy- (or undeploy) command to initiate policy undeployment. The command executes selang commands stored with the RULESET object that is associated with the POLICY object you are deploying. These are policy undeployment commands.

#### **WARNING**

We strongly recommend that you use the policydeploy utility to undeploy a policy. The deploy- command only executes part of the policy undeployment and does not update the DMS when undeploying a policy from an endpoint.

To run this command, you need to have:

- Sub-administration rights for the POLICY, HNODE, and RULESET classes on each database in the hierarchy below the database where you undeploy the policy.
- Appropriate sub-administration rights on each database in the hierarchy below the database where you undeploy the policy.

These are the permissions necessary to execute the selang commands that form the policy undeployment script on each of these computers.

#### **NOTE**

For more information about deploying a policy, see the *Enterprise Administration Guide*.

This command has the following format:

```
{deploy-|undeploy} POLICY name#xx
```

- *name#xx*  
The name of the POLICY object (policy name and version number) for the policy you want to undeploy.

## editfile Command Create and Modify File Records

### Valid in the AC environment

This command is documented with the chfile command.

## edit x grp Command Create and Modify Group Records

### Valid in the AC environment

This command is documented with the ch[x]grp command.

## editres Command Modify Resource Records

### Valid in the AC environment

This command is documented with the chres command.

## edit x usr Command Modify User Records

### Valid in the AC environment

This command is documented with the chxusr command.

## end\_transaction Command Complete Recording Dual Control Transactions

### Valid on UNIX hosts in the AC environment

The end\_transaction command completes the start\_transaction command for Dual Control PMDB processes.

## environment Command Set the Security Environment

### Valid in all environments

The environment command sets the security environment. Privileged Access Manager supports the Privileged Access Manager and UNIX security environments. When the selang command shell is invoked, the AC environment is selected by default.

This command has the following format:

```
environment {ac|config|etrust|native|nt|pmd|seos|unix}
```

- **ac**  
Specifies the Privileged Access Manager security environment. The selang commands affect the local Privileged Access Manager database. Some commands support simultaneous updates to the native OS security settings of the host you are connected to. In the Privileged Access Manager environment, the selang prompt is as follows:

```
PAMSC>
```

- **config**  
Specifies the remote configuration environment, which lets you change endpoint configuration settings.
- **etrust**  
Specifies the Privileged Access Manager security environment.

#### NOTE

This is the same as specifying AC and is maintained for compatibility with older versions.

- **native**  
Specifies the native operating system security environment (either Windows or UNIX) of the host you are connected to, whether local or remote. The selang commands affect the native OS database. In the native environment, the selang prompt is:

```
PAMSC (native)>
```

- **nt**  
Specifies the Windows security environment. The selang commands affect the Windows database. Some commands support simultaneous updates to the Privileged Access Manager security settings. In the Windows environment, the selang prompt is:

```
PAMSC (nt)>
```

- **pmd**  
Specifies the selang commands in the remote management environment. When the selang command shell is set to the pmd environment, the commands operate on the PMDB of the selected host. In the pmd environment, the selang prompt is as follows:

PAMSC (pmd) >

- **seos**  
Specifies the Privileged Access Manager security environment.

**NOTE**

This is the same as specifying *AC* and is maintained for compatibility with older versions.

- **unix**  
Specifies the UNIX security environment. The *selang* commands operate on the UNIX security system. In the UNIX environment, the *selang* prompt is as follows:

PAMSC (unix) >

## find Command List Database Records

### Valid in AC and native environments

The *find* command displays the names of records in a specified class. If you do not specify any parameters, it displays the names of all classes.

**NOTE**

The *find* command is identical to the commands *list* and *search*.

To use this command you must have sufficient authority, as defined by the following conditions:

- If you have the ADMIN, AUDITOR, or OPERATOR attribute, you can use the *find* command with all parameters.
- If you have READ authority for a record in the ADMIN class, you can specify the class parameter for the class represented by the record.

This command has the following format:

```
{find|f|list|search} [{className|class(className)}] [objName]
```

- *className*  
Specifies the class within which *find* searches for records. If *className* is not provided, *find* lists all classes.
- *objName*  
Specifies the records that Privileged Access Manager searches for. *objName* can include wildcard characters.

### Example: Display all Records in the TERMINAL Class

To display all the members in the TERMINAL class, enter the following command:

```
find terminal
```

## get dbexport Command Retrieve Exported Database Rules

### Valid in the AC environment

The *get dbexport* command retrieves the rules that were exported from the Privileged Access Manager database or PMD database on the host you are connected to. For the exported database to exist, you must issue the *start dbexport* command before you issue the *get dbexport* command.

This command has the following format:

```
get dbexport [pmdname(name)] [params(OFFSET=number)]
```

- `pmdname(name)`  
(Optional) Defines the name of the PMD database that you exported.
- `params(OFFSET=number)`  
(Optional) Defines the offset for retrieving more lines from the database output. The `get dbexport` command can only return 200 lines from the exported database per request. If there is more information in the output, the command returns offset data that specifies the last line returned.

### Example: Retrieve rules from an exported database

The following example shows how the `get dbexport` command is used to retrieve information from the exported Privileged Access Manager database on the host you are connected to. The first command retrieves the first 200 lines and the second command retrieves the following 200 lines of the output:

```
PAMSC> get dbexport

(localhost)

Data for DBEXPORT 'seosdb'

-----

setoptions class+(CLASS)setoptions class+(CLASS)

setoptions class+(CLASS)

...

chres CLASS ("resource") defaccess(none)

OFFSET:      201
```

```
PAMSC> get dbexport params("offset=201")

(localhost)

Data for DBEXPORT 'seosdb'

-----

chres CLASS ("resource") defaccess(none)

chres CLASS ("resource") defaccess(none)

chres CLASS ("resource") defaccess(none)

...
```

```
chres CLASS ("resource") defaccess(none)

OFFSET:      401
```

## get devcalc Command Retrieve Policy Deviation Data

### Valid in the AC environment

The get devcalc command retrieves information from the policy deviation data file (deviation.dat) that contains policy deviation calculation results and sends it to one or more set DMS databases. For the data file to exist, the start devcalc command must have been issued before.

When you create a policy or host report, you can also specify to include deviation calculation results. The reporting utility then issues this command.

#### WARNING

The deviation calculation does not check whether native rules are applied. It also ignores rules that remove objects (user or object attributes, user or resource authorization, or actual users or resources) from the database. For example, the calculation cannot verify whether the following rule is applied:rr SUDO admCommand

#### NOTE

For more information about the policy deviation data file and advanced policy reporting, see the *Enterprise Administration Guide*.

To run the get devcalc command you must have terminal access rights to the computer and read access to DEVCALC sub-administration class.

This command has the following format:

```
get devcalc [params("offset=number")]
```

- **offset=number**  
(Optional) Defines the offset for retrieving more lines from the policy deviation data file. The get devcalc command can only return a maximum number of lines (set by the max\_lines\_request configuration setting) from the policy deviation data file per request. If there is more information in the file, the command returns offset data that specifies the last line returned.

### Example: Get policy deviation data

The following example shows how the get devcalc command is used to retrieve information from the policy deviation data file when the max\_lines\_request setting is set to 10. The first command retrieves the first ten lines and the second command then retrieves the following ten lines of the output:

```
PAMSC> get devcalc

(localhost)

Data for DEVCALC 'deviation'

-----
```

---

DATA : DATE, Mon Mar 20 11:22:15 2006

POLICYSTART, myPolicy#01

DIFF, (FILE), (file1), (\*), (\*)

DIFF, (FILE), (file2), (\*), (\*)

DIFF, (FILE), (file3), (\*), (\*)

DIFF, (FILE), (file4), (\*), (\*)

DIFF, (FILE), (file5), (\*), (\*)

DIFF, (FILE), (file6), (\*), (\*)

DIFF, (FILE), (file7), (\*), (\*)

OFFSET : 11

PAMSC> get devcalc params("offset=11")

(localhost)

Data for DEVCALC 'deviation'

-----

DATA : DIFF, (FILE), (file8), (\*), (\*)

DIFF, (FILE), (file9), (\*), (\*)

DIFF, (FILE), (file10), (\*), (\*)

DIFF, (FILE), (file11), (\*), (\*)

DIFF, (FILE), (file12), (\*), (\*)

DIFF, (FILE), (file13), (\*), (\*)

DIFF, (FILE), (file14), (\*), (\*)

DIFF, (FILE), (file15), (\*), (\*)

DIFF, (FILE), (file16), (\*), (\*)

DIFF, (FILE), (file17), (\*), (\*)

OFFSET : 21

## help Command Get selang Help

### Valid in all environments

The help command displays selang syntax in several ways:

- Used without parameters, it displays a list of the selang commands, with a brief explanation of each.
- Used with a selang command name, it displays the syntax of the given command.
- Used with the access parameter, it displays a list of values for the access parameter of the authorize command and the defaccess parameter of the new\*, ch\*, and edit\* commands.
- Used with the lineedit parameter, it displays a list of special characters for selang command line manipulations.

#### NOTE

To display the help text for a command typed in the command line without deleting the text in the command line, type Ctrl+2.

```
{help|h} [commandName|access|lineedit|className|properties|privilege]
```

- **access**  
Requests a class-by-class list of the access types that the access and defaccess parameters can specify.
- **className**  
Requests a short description of the specified class.
- **command-name**  
Requests the syntax for the specified command.
- **lineedit**  
Requests a list of special characters for selang command line manipulations.
- **properties**  
(AC environment) Requests information on how to update user-defined properties.
- **privilege**  
(Windows environment) Requests a list of possible Windows privileges for the ch[x]grp, ch[x]usr, edit[x]grp, and edit[x]usr commands.

## history Command Show Previously Issued Commands

### Valid in all environments

The history command lists all the commands that were entered during the current selang command shell session. The commands are ordered chronologically. Each command is preceded by the number of the command. For example, the third command entered is preceded by the number three.

The history command does not display a password even if one was entered as part of a ch[x]usr, new[x]usr, or edit[x]usr commands. The history command displays a series of asterisks (\*\*\*) instead of the clear text password.

This command has the following format:

```
history
```

## hosts Command Connect to a Remote Terminal

### Valid in all environments

The hosts command specifies the hosts or Policy Models to which the selang commands are sent. It lets you connect to a remote Privileged Access Manager computer with a different name, so you can remotely manage the computer while local Privileged Access Manager services are running. By default, all selang commands are directed to the database on the local host.

The hosts command must be executed before executing the commands that are to be directed to the hosts.

To administer (update) a remote host database from the local host, you must meet *one* of the following criteria:

- Be explicitly authorized to update the remote host database from the local database
- Be a member of a group that is allowed to update the remote host database from the local database
- Be the owner of the local host as defined in the remote host

To list all the hosts and PMDBs that are currently available, specify the hosts command without any parameters.

#### NOTE

Privileged Access Manager protects hosts through their canonical host names and not through aliases. To avoid the confusion caused by alias names, Privileged Access Manager issues a warning when a HOST rule is defined for an alias name. Similarly, Privileged Access Manager gives a warning if a HOST is defined with less than a fully qualified name, because Privileged Access Manager uses fully qualified names (for example, mymachine.yourcompany.com) for hosts.

This command has the following format:

```
hosts [{systemIds|policyModel@[hostname]]} [uid(username) password(pw)]
```

- **systemIds**  
Specifies the system IDs of the hosts on which the selang commands are to be executed. When specifying more than one host, enclose the list of systems IDs in parentheses and separate the system IDs with a space or a comma.
- **policyModel@[hostname]**  
Specifies the addresses of the Policy Models on which the selang commands are to be executed. When specifying more than one Policy Model, enclose the list of Policy Model addresses in parentheses and separate the Policy Model addresses with a space or a comma.  
**Default:** If you do not specify *hostname*, Privileged Access Manager tries to connect to the PMDB on the local host.

#### NOTE

The advantage of using a Policy Model over explicitly specifying the hosts is that the system where the Policy Model resides keeps on trying to update all the systems defined to the Policy Model, even if they are currently unavailable. For more information about Policy Models, see the *Endpoint Administration Guide* for your OS.

- **uid(username)**  
(Optional) Specifies the name of an alternate Privileged Access Manager admin that may be used to log into the target database.
  - **password(pw)**  
Specifies the password of the user ID in the uid token.

#### Example: Connect to the Local Host

To connect to the local seosdb database, use the following command:

```
hosts @
```

To connect to a local PMDB, use the following command:



```
hosts PMDB@
```

**Example: Let a User or Group Update Remote Hosts**

To give a user authorization to update the remote host database from the local database, on the remote host enter the command:

```
authorize TERMINAL local_host uid user_name access(write)
```

To give a group authorization to update the remote host database from the local database, on the remote host enter the command:

```
authorize TERMINAL local_host gid(group_name) access(write)
```

**Example: Apply selang Commands to a Remote Policy Model**

To apply all subsequent commands to the Policy Model on the station h1, type the command:

```
hosts Policy@h1
```

If the connection to *Policy@h1* is successful, the following message appears.

```
Successfully connected to h1
```

All commands entered from now on are directed to *Policy@h1* and not to the local host. The selang prompt changes to the following:

```
Remote_PAMSC>
```

**Example: Apply selang Commands to a Remote Host**

To apply all future commands to the station athena, type the command:

```
hosts athena
```

If successful connections are made to athena, the following messages appear on the screen.

```
(athena)
```

```
Successfully connected
```

```
INFO: Target version is 2.50
```

Any command you enter is applied to athena and is not sent to the local host. If you add a new user, the user is only added to athena, as shown in this example:

```
Remote_PAMSC>newusr steve

(athena) USER steve successfully added.
```

### Example: Connect as a Different User

You can use the uid and password parameters to log into the database (seosdb or PMDB) as a different user. This is useful when connecting to the local or remote host as administrator (root).

```
hosts @ uid(root) password(P@ssword01)
```

## join x Command Add Users to Internal Groups

### Valid in the AC environment

The join[x] command adds users to one or more internal groups, or changes the users' properties with respect to the groups. The specified users and groups must already be defined to Privileged Access Manager.

Use join to add internal users to groups.

Use joinx to add enterprise users to groups.

#### NOTE

This command also exists in the native environment but operates differently there.

The set of properties from the join command *completely replaces* any previous set of properties for the specified users in the specified groups. If any such properties were defined earlier, they are not retained unless the new join command specifies them again.

#### NOTE

For more information about group properties, see the *Endpoint Administration Guide* for your OS.

You can use the join command if at least one of the following conditions is true:

- You have the ADMIN attribute.

#### NOTE

If you want to modify Privileged Access Manager GROUP records *and* enterprise groups you need both the MODIFY and JOIN access authority.

- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group.
- You are assigned CONNECT authority in the access control list of the GROUP record in the ADMIN class.

This command has the following format:

```
{join[x]|j[x]} {userName|(userName [,userName...])} \
group(groupName [,groupName...]) \
[admin|admin-] \
[auditor|auditor-] \
[gowner(group-name)] \
[operator|operator-] \
```

```
[owner(userName|groupName)] \
[pwmanager | pwmanager-] \
[regular] \
[nt | unix]
```

- **admin**  
Assigns the GROUP-ADMIN attribute to the user specified by *userName*.
- **admin-**  
Removes the GROUP-ADMIN attribute from the user.
- **auditor**  
Assigns the GROUP-AUDIT attribute to the user specified by *userName*.
- **auditor-**  
Removes the GROUP-AUDIT attribute from the user.
- **gowner(groupName)**  
Specifies that the user is being added to the group *groupName*.
- **group(groupName [,groupName...])**  
Specifies the group or groups to which the that the user is being added as a member.
- **nt**  
Connects *userName* to a group in the Windows database.
- **operator**  
Assigns the GROUP-OPERATOR attribute to the user specified by *userName*.
- **operator-**  
Removes the GROUP-OPERATOR attribute from the user.
- **owner(Name)**  
Specifies a Privileged Access Manager user or group as the owner of the join record. If you are creating a connection and you do not specify an owner, you are the owner of the connection.
- **pwmanager**  
Assigns the GROUP-PWMANAGER attribute to the user specified by *userName*.
- **regular**  
Resets the administrative flags for the user.
- **unix**  
Connects *userName* to the group in the UNIX security system.
- **userName**  
Specifies a user who is to be connected (or reconnected with a new set of properties) to the group or groups specified by the group parameter.  
If the command is join, *userName* is the name of a USER record. If the command is joinx, *userName* is the name of an enterprise user.

## Examples

- The user Rorri wants to join the user Bob to the internal group staff.
  - Rorri has the ADMIN attribute.
  - The following defaults apply:
    - admin
    - auditor
    - owner(Rorri)
    - pwmanager

```
join Bob group(staff)
```
- The user Rorri wants to change the definition of Sue in the group staff. She currently is a GROUP-AUDITOR; Rorri wants to add the GROUP-PWMANAGER attribute.

- Rorri has the ADMIN attribute.
- The following defaults apply:
  - admin
  - owner(Rorri)

```
join Sue group(staff) auditor pwmanager
```

When selang executes this command, it deletes the previous record. No record is kept of Sue's previous attributes. Therefore, Rorri must specify the two attributes Sue should have now.

## join x - Command Remove Users from Groups

### Valid in the AC environment

The join[x]- command removes users from internal groups.

join- removes internal users from internal groups.

joinx- removes enterprise users from internal groups.

#### NOTE

The join[-] command also exists in the native environment but operates differently there.

To use the join[x]- command, one of the following conditions must be true:

- You have the ADMIN attribute.

#### NOTE

If you want to modify Privileged Access Manager GROUP records *and* native groups you need both the MODIFY and JOIN access authority.

- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group.
- You are assigned CONNECT authority in the access control list of the GROUP record in the ADMIN class.

This command has the following format:

```
{join[x]-|j[x]-} {userName| (userName [,userName...])} \
group(groupName [,groupName...])
```

- **group(groupName [,groupName...])**  
Specifies the group or groups from which to remove the user.
- **userName**  
Specifies the user you want to remove from the group.  
If the command is join, *userName* is the name of a USER record.  
If the command is joinx, *userName* is the name of an enterprise user.

### Example

The user Bill wants to remove the users sales25 and sales43 from the group PAYROLL.

The user Bill has the ADMIN attribute.

```
joinx- (sales25 sales43) group(PAYROLL)
```

## newfile Command Create File Records

### Valid in the AC environment

This command is documented with the chfile command.

## new x grp Command Create Group Records

### Valid in the AC environment

This command is documented with the chgrp command.

## newres Command Create Resource Records

### Valid in the AC environment

This command is documented with the chres command.

## new x usr Command Create User Records

### Valid in the AC environment

This command is documented with the ch[x]usr command.

## rename Command Rename a Database Record

### Valid in the AC environment

Renames a record name in the database. The record is now known by its new name only.

#### NOTE

You cannot rename records in the SEOS, UACC, and ADMIN classes.

To use the rename command, you must have sufficient authority over the record. Privileged Access Manager makes the following checks until one of the conditions is met:

- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the record.
- You are assigned CREATE (for editres) access authority in the access control list of the resource class's record in the ADMIN class.

This command has the following format:

```
rename classNameoldresourceNamenewresourceName
```

- *className*  
Defines the class to which the record you want to rename belongs.
- *oldresourceName*  
Defines the current name of the record in Privileged Access Manager.
- *newresourceName*  
Defines the new name you want to assign to the record.

### Example

The user ADMIN 1 wants to rename the record *spree3* in class Host to *spree4*.

- The security administrator has the ADMIN attribute.

```
rename host spree3 spree4
```

## rmfile Command Delete File Records

### Valid in the AC environment

The rmfile command deletes records belonging to the FILE class from the database.

You can delete a file record if one of the following conditions is met:

- You have the ADMIN attribute.
- The record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the file.
- You have the DELETE access authority assigned in the ACL of the FILE record in the ADMIN class.

This command has the following format:

```
{rmfile|rf} {fileName | (filename [,filename...])}
```

- *fileName*  
Defines the file you are removing.  
Privileged Access Manager processes each file record independently. If an error occurs while processing a file, Privileged Access Manager issues a message and continues processing with the next file in the list.

### Example: Remove File Protection

The security administrator (which has the ADMIN attribute) wants to remove Privileged Access Manager protection for a file. On UNIX, this can look like this:

```
rmfile /etc/passwd
```

The same command on Windows can look like this:

```
rmfile C:\temp\passwords.txt
```

## rm x grp Command Delete Group Records

### Valid in the AC environment

The rmgrp and rmxgrp commands remove one or more groups from Privileged Access Manager and, optionally, from the native environment.

#### NOTE

There may be occurrences in the database of the group's group ID that the rmgrp command does not delete. For example, the group could be the owner of another group, the owner of other records, or in an access control list for a resource. Use the chgrp, chusr, chres, and authorize commands, as required, to manually change ownership and remove access authorities relating to the group record you want to delete. Alternatively, use the sepurgedb utility to clean up inconsistencies in the database automatically.

#### NOTE

The rmgrp command also exists in the native environment but operates differently there.

To use the rmgrp command, at least one of the following is required:

- You have the ADMIN attribute.
- The group to be deleted is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group to be deleted.
- You are assigned DELETE authority in the GROUP record of the AUDIT class.

This command has the following format:

```
{rmgrp|rg | rmxgrp|rxg} { groupName | (groupName [,groupName...]) } [unix|nt]
```

- *groupName*  
Specifies the Privileged Access Manager group to be deleted.
- **nt**  
(Optional) Deletes a group from the local Windows database in addition to deleting the group from the Privileged Access Manager database.
- **unix**  
(Optional) Deletes a group from the local UNIX system in addition to deleting the group from the Privileged Access Manager database.

### Example

The user Joe wants to delete the groups DEPT1 and DEPT2 from the database.

- The user Joe has GROUP-ADMIN authority to the SALES group.
- The groups DEPT1 and DEPT2 are owned by the SALES group.

```
rmxgrp (DEPT1, DEPT2)
```

## rmres Command Delete a Resource

### Valid in the AC environment

The `rmres` command removes resources from the database. Records belonging to the following classes can be deleted using the `rmres` command: ACVAR, ADMIN, APPL, CATEGORY, CONNECT, FILE, GAPPL, GHOST, GSUDO, GTERMINAL, HNODE, HOST, HOSTNET, HOSTNP, LOGINAPPL, MFTERMINAL, POLICY, PWPOLICY, SECFILE, SECLABEL, SPECIALPGM, SUDO, SURROGATE, TERMINAL, PROGRAM, PROCESS, RULESET, TCP, UACC, and any user defined class.

#### NOTE

This command also exists in the native Windows environment but operates differently.

To remove a record from the database, you must meet one of the following conditions:

- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the resource record.
- You are assigned the DELETE authority in the access control list of the resource class's record in the ADMIN class.

This command has the following format:

```
{rmres|rr} classNameresourceName
```

- *className*  
Specifies the name of the class to which the resource belongs. To list the resource classes defined to Privileged Access Manager, use the `find` command. See the `find` command in this chapter for more information.
- *resourceName*  
Specifies the name of the resource record you are deleting. When removing more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma.  
Privileged Access Manager processes each resource record independently. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.

### Example

The user Admin1 wants to remove the record TERMS from the TERMINAL class in the database.

- The user Admin1 has the ADMIN attribute.

```
rmres TERMINAL TERMS
```

## rm x usr Command Delete User Records

### Valid in the AC environment

The `rmusr` and `rmxusr` commands remove users from the Privileged Access Manager database, and also remove references to the user's record that exist in Privileged Access Manager group records.

`rmxusr` removes an enterprise user from the Privileged Access Manager database. `rmusr` removes an internal user from the database. The `rmusr` command can, optionally, remove the user from the native environment as well.

#### NOTE

There may be occurrences in the database of the user that `rm[x]usr` does not delete. For example, the user could be the owner of a group, the owner of other records, or in an access control list for a resource. Use the `ch[x]grp`, `ch[x]usr`, `ch[x]res`, and `authorize` commands, as required, to manually change ownership and remove access authorities relating to the user record you want to delete. Alternatively, use the `sepurgedb` utility to clean up inconsistencies in the database automatically.

#### NOTE

The `rmusr` command also exists in the native environment but operates differently there.

To execute the `rm[x]usr` command you need to meet at least one of the following requirements:

- You have the ADMIN attribute.
- The user record to be deleted is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are assigned the DELETE authority in the access control list of the USER record in the ADMIN class.
- You are the owner of the user record.

`ru` is a synonym of `rmusr`.

`rxu` is a synonym of `rmxusr`.

This command has the following format:

```
{rmusr|ru | rmxusr | rxu} { userName | (userName [,userName...]) } \
[unix|nt] [appl(homedir=yes)]
```

- **appl(homedir=yes)**  
(UNIX only). Deletes the user's home directory  
This argument checks for the existence of the user's home directory in `/home`, `/tmp` or `/users`. If the home directory located in another directory, edit the `S99DELETE_postrmusrdir.sh` script to incorporate it.

#### NOTE

You must specify the `unix` option before you specify this option.

- **nt**  
Deletes the user from the Windows environment, in addition to deleting the user from Privileged Access Manager.  
Valid only for `rmusr`.
- **userName**  
Defines a user record.
- **unix**  
Deletes the user from the UNIX environment, in addition to deleting the user from Privileged Access Manager.  
Valid only for `rmusr`.

### Example

The following command deletes enterprise users Terry and Jane from Privileged Access Manager:

```
rxu (Terry, Jane)
```



## ruler Command Select Properties to Display

### Valid in AC and native environments

The ruler command defines the ruler for a class, and so lets you define the set of properties of a class that Privileged Access Manager displays.

The ruler command only applies to the hosts of the current session. The properties of each host are displayed in a separate list. If you change hosts, the ruler command does not change the display of properties in the new hosts.

The following users can issue this command:

- Users with the ADMIN, AUDITOR, or OPERATOR attribute.
- Users who have access read in class ADMIN for the class whose ruler they are trying to set. For example, if you have access read in class ADMIN for the record representing class TERMINAL, you can set the ruler for class TERMINAL.

This command has the following format:

```
ruler className [props( all | propertyName [,propertyName...])]
```

- *className*  
The name of the class whose display you want to change.
- [props(all | *propertyName* [,*propertyName*...])]  
Specifies the properties to be displayed.  
If you omit the props parameter, Privileged Access Manager displays the names of the properties that are in the current ruler.
  - **all**  
Specifies that all the properties of the class to be displayed.
  - *propName*  
Specifies a Privileged Access Manager property to be displayed. You can specify up to 40 properties, separated by spaces or commas.

### Examples

- The user admin wants Privileged Access Manager to display only two properties for each user: the owner and the user who is notified about changes.

```
ruler USER props(NOTIFY, OWNER)
```

- The user admin wants to display the properties in the current ruler for class USER.

```
ruler USER
```

- The user admin wants Privileged Access Manager to revert to the default ruler, which is to display all the properties in the class USER.

```
ruler USER props(all)
```

## setoptions Command Set Options

### Valid in the AC environment

The setoptions command sets system-wide Privileged Access Manager options in the running system. For example, you can use setoptions to:

- Enable or disable security checking for each class, or for all classes
- Set the password policies
- List the current settings of the Privileged Access Manager options

#### NOTE

This command also exists in the Windows environment, but operates differently there.

You need the ADMIN attribute to use the setoptions command. However, you only need the AUDITOR or OPERATOR attribute to use the command setoptions list.

This command has the following format:

```
{setoptions|so} \
[accgrr|accgrr-] \
[accpacl|accpacl-] \
[ac_id(id)] \
[class+ (className)] \
[class- (className)] \
[class (className)] \
[flags{+|-} (I|W)] \
[cng_adminpwd|cng_adminpwd-] \
[cng_ownpwd|cng_ownpwd-] \
[cwarnlist] \
[dms{+|-} (dms@hostname)] \
[inactive(nDays)|inactive-] \
[is_dms{+|-}] \
[list] \
[maxlogins (nLogins)|maxlogins-] \
[password( \[{history(nStoredPasswords) | history-}] \[(interval(nDays) | interval-)] \[(min_life(nDays) |
min_life-)] \[{rules( \ [alpha(nCharacters)] \ [alphanum(nCharacters)] \ [(bidirectional) | (bidirectional-)]
\ [grace(nLogins)] \ [lowercase(nCharacters)] \ [min_len(nCharacters)] [max_len(nCharacters)]
\ [max_rep(nCharacters)] \ [{namechk|namechk-}] [numeric(nCharacters)] \ [{oldpwchk|oldpwchk-}]
[prohibited(prohibitedCharacters)] \ [special(nCharacters)] \ [sub_str_len(nCharacters)] \
[uppercase(nCharacters)] \ [use_dbdict|use_dbdict-] \)|rules-}] \
)] \
```

- **accgrr**  
Enables the accumulative group rights (ACCGRR) option.  
The default value is enabled.
- **accgrr-**  
Disables the accumulative group rights (ACCGRR) option.
- **accpacl**  
Enables the use of PACLs in all resources.
- **accpacl-**  
Disables the use of PACLs.
- **ac\_id(id)**  
Defines a unique ID for the endpoint (HNODE object) that is saved in the local Privileged Access Manager database and on the DMS. Privileged Access Manager uses this ID to identify the HNODE, so that changes to the endpoint's IP address or name do not affect advanced policy management functionality; Privileged Access Manager can still trace the endpoint.
- **class (className)**  
Sets or clears a setting for a Privileged Access Manager class.
- **class+(className)**  
Enables one or more Privileged Access Manager classes. A class must be enabled for Privileged Access Manager to protect resources of that class. A class should be activated only after you have defined the necessary records to allow access to the resources that belong to the class. See the *Endpoint Administration Guide for UNIX* for more information about the resource classes supplied with Privileged Access Manager.  
Use one of the following values:

- The name of a Privileged Access Manager class
- SECLEVEL. This enables security level checking.
- PASSWORD. This activates the password rules. On Windows, it also enables arbitrarily long passwords.
- **class-(className)**  
Disables one or more Privileged Access Manager classes. Resources that belong to a disabled class are not protected by Privileged Access Manager. Use one of the following values:
  - The name of a class
  - SECLEVEL. This disables security level checking.
  - PASSWORD. This disables the password rules. On Windows, this also disables the long passwords.
 You cannot disable the classes GROUP, SECFILE, SEOS, UACC, and USER.
- **cng\_adminpwd**  
Enables users with the PWMANAGER attribute to change the ADMIN user's password.
- **cng\_adminpwd-**  
Disables users with the PWMANAGER attribute from changing the ADMIN user's password. This is the default setting.
- **cng\_ownpwd**  
Enables users to change their own passwords through selang.
- **cng\_ownpwd-**  
Disables users from changing their own passwords through selang. This is the default setting.
- **cwarnlist**  
Displays a table with data about which classes are in Warning mode.
- **dms{+|-}(dms@hostname)**  
Adds or removes DMS databases from the list of DMS databases for this database.
- **flags{+|-} (I|W)**  
Sets or clears functionality that is associated with a class. Valid values are:
  - **I**  
Case-sensitivity for objects in the specified class.
 

**NOTE**  
Verify that there is a resource with the same name before setting I flag. Privileged Access Manager shows a database error on restarting, if there are multiple upper or lower case resources. Restart Privileged Access Manager for the I flag change to take effect.
  - **W**  
Warning mode for the specified class.
 

**NOTE**  
Flags are case-sensitive; use uppercase letters.
- **history(NStoredPasswords)**  
Specifies the number of previous passwords that are stored in a history list. When a password is changed, the previous password is added to the list, and the oldest password is dropped from the list if necessary. Privileged Access Manager prevents a user from changing their password to one that is in the list.  
Enter an integer from 1 through 24. If you specify zero, no passwords are saved.  
On Windows, the history option enables the use of passwords longer than eight characters. The setoptions bidirectional or bidirectional- option determines the form of encryption used when storing the password.  
On UNIX, the history option does *not* affect whether long passwords are enabled. Use the passwd\_local\_encryption\_method configuration setting to determine whether long passwords are enabled.
- **history-**  
Disables password history checking.  
On Windows, this option disables the use of long passwords.
- **inactive(nDays)**

Specifies the number of inactive days after which a user's login is suspended. An inactive day is a day when the user does not log in. Enter a positive integer. If inactive is set to zero, the effect is the same as using the inactive-parameter.

- **inactive-**  
Disables the inactive login check.
- **interval(*nDays*)**  
Sets the number of days that must pass after passwords are set or changed before the system prompts users for a new password. Enter a positive integer or zero. An interval of zero disables password interval checking for users. Set the interval to zero if you do not want passwords to expire.  
If the utility `segrace` is part of the user's login script, Privileged Access Manager informs the users that the current password has expired when the specified number of days is reached. The users can immediately renew the password or continue using the old password until the number of grace logins is reached. After the number of grace logins is reached, the users are denied access to the system and must contact the system administrator to select a new password.
- **interval-**  
Cancels the password interval setting.
- **is\_dms+**  
Designates the current database as a DMS.
- **is\_dms-**  
Removes the designation of the current database as a DMS.
- **list**  
Displays the current settings on the screen.
- **maxlogins(*nLogins*)**  
Sets the maximum number of terminals the user can log in to at the same time. A value of 0 (zero) means that the user can log in from any number of terminals concurrently. This value can be overridden by assigning a value in the user's user record.

**NOTE**

If maxlogins is set to 1, you cannot run `selang`. You must shut down Privileged Access Manager, change the maxlogins setting to greater than one, and restart Privileged Access Manager.

**NOTE**

Valid only on Unix and Linux operating systems.

- **maxlogins-**  
Disables the global maximum logins check. The number of terminals a user can log in is from unlimited, unless the user's login is restricted in the user record of the user.
- **min\_life(*NDays*)**  
Sets the minimum number of days between password changes. Enter a positive integer.
- **password**  
Sets the password options.
- **rules**  
Sets one or more password rules that Privileged Access Manager uses to check the quality of new passwords. The rules are:
  - **alpha(*nCharacters*)**  
Sets the minimum number of alphabetic characters the new password must contain. Enter an integer.
  - **alphanum(*nCharacters*)**  
Sets the minimum number of alphanumeric characters the new password must contain. Enter an integer.
  - **bidirectional**  
Specifies that when passwords are sent to other systems as part of PMDB, they are distributed in clear text (within encrypted messages).  
On UNIX, this option is equivalent to setting the following passwd section setting value:

```
Passwd_distribution_encryption_mode=bidirectional
```

#### NOTE

We recommend that you set the configuration setting rather than use the `setoptions` command.

On Windows, the passwords are stored in the history list with the encryption specified in the registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Encryption Package
```

#### – **bidirectional-**

Specifies that passwords are sent in their hash encrypted form.

On Windows the hash function used is SHA-1.

On UNIX, this option is equivalent to setting the following `passwd` section setting value:

```
Passwd_distribution_encryption_mode=compatibility
```

#### NOTE

We recommend that you set the configuration setting rather than use the `setoptions` command.

If this option is specified, long passwords cannot be distributed between heterogeneous operating systems.

#### – **grace(*nLogins*)**

Sets the maximum number of grace logins that are permitted before the user is suspended. The number of grace logins must be from 0 through 255 inclusive.

#### – **lowercase(*nCharacters*)**

Sets the minimum number of lowercase characters the new password must contain. Enter an integer.

#### – **min\_len(*nCharacters*)**

Sets the minimum password length. Enter the minimum total number of characters that the new password must contain.

#### – **max\_len(*nCharacters*)**

Sets the maximum password length. Enter the maximum total number of characters that the new password must contain.

#### – **max\_rep(*nCharacters*)**

Sets the maximum number of repetitive characters the new password must contain. Enter an integer.

#### – **namechk**

Checks whether the password contains or is contained by the user's name. By default, Privileged Access Manager performs this check.

#### – **namechk-**

Turns off the `namechk` check.

#### – **numeric(*nCharacters*)**

Sets the minimum number of numeric characters the new password must contain. Enter an integer.

#### – **oldpwchk**

Checks whether the new password contains or is contained by the password being replaced. By default, Privileged Access Manager performs this check.

#### NOTE

Valid only on Unix and Linux operating systems.

#### – **oldpwchk-**

Turns off the `oldpwchk`.

#### – **prohibited(*prohibitedCharacters*)**

Specifies characters a user cannot use in a password. Enter the prohibited characters.

#### NOTE

We recommend you to verify that control characters '\ ' and 't' are both specified in the `prohibitedCharacters` list, to block the use of the tab key.

#### – **special(*nCharacters*)**

Sets the minimum number of special characters the new password must contain. Enter an integer.

#### – **sub\_str\_len(*nCharacters*)**

- Sets the maximum number of characters the new password can share with the previous password. Enter an integer.
- **uppercase(*nCharacters*)**  
Sets the minimum number of uppercase characters the new password must contain. Enter an integer.
- **use\_dbdict | use\_dbdict-**  
Sets the password dictionary. use\_dbdict sets the token to db and compares passwords against words in the Privileged Access Manager database. use\_dbdict- sets the token to file and checks passwords against a file specified in the seos.ini file for UNIX or Windows registry for Windows.
- **rules-**  
Disables password quality checking. None of the rules specified by the rules argument are used for password quality checking.

### Examples: Set Privileged Access Manager Options

- The user John wants to activate the OpsAct class, an installation-defined class used to protect operator actions. The user John has the ADMIN attribute.  

```
setoptions class+(OpsAct)
```
- The user Mike wants to set a password policy that forces users to supply passwords of length at least 6 characters. Mike also wants to activate password policy enforcement. The user Mike has the ADMIN attribute.  

```
setoptions class+(PASSWORD)
setoptions password(rules(min_len(6)))
```
- The user SecAdmin wants to enable security level checking. The user SecAdmin has the ADMIN attribute.  

```
setoptions class+(SECLEVEL)
```
- The user Janani wants to set a DMS for this database to send notification to. The user Janani has the ADMIN attribute.  

```
setoptions dms+(apache@myHost)
```

### Example: Put a Class into Warning Mode

Put a class into Warning mode by setting the Warning property on the class. You can use the setoptions selang command to do this, as follows:

```
setoptions class(classname) flags+ (W)
```

- **classname**  
Defines the name of the class you want to put into Warning mode.

#### NOTE

The W flag is case-sensitive and must be in uppercase.

To clear Warning mode for the class, you can also use the setoptions command, as follows:

```
setoptions class(classname) flags- (W)
```

### search Command List Database Records

#### Valid in AC and native environments

This is identical to the find command.

### showfile Command Display File Properties

#### Valid in the AC environment

The showfile command lists the properties of a file record. The properties are listed in alphabetical order. Privileged Access Manager processes each record independently and displays information only for those resources for which you have sufficient authority.

### NOTE

This command also exists in the native environment but operates differently there.

To execute a showfile command, at least one of the following conditions is required:

- You have at least one of the following attributes: ADMIN, AUDITOR, and OPERATOR.
- You are the owner of the file.
- You are assigned read authority in the access control list of the object representing the FILE class record in the ADMIN class.
- You have the GROUP-ADMIN or GROUP-AUDITOR attribute in the group that owns the file or that is a parent of the group that owns the file.

This command has the following format:

```
{showfile|sf} {fileName |(fileName [,fileName...])} \
[addprops(propName [,propName ...])] \
[next] \
[props(all | propName [,propName ...])] \
[useprops(propName [,propName ...])] \
[nt|unix]
```

- **addprops(propName [,propName ...])**  
Defines properties to be added to the class ruler for this query only.
- **fileName**  
Specifies the name of the file record whose properties are to be listed.  
Privileged Access Manager processes each file record independently. If an error occurs while processing a file, Privileged Access Manager issues a message and continues processing with the next file in the list.  
*fileName* can contain wildcard characters, and so match multiple file names.  
On UNIX, to display the properties of a file whose name contains a special character or space, type an extra slash (/) before the file name.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size.  
The maximum query size is determined by the query\_size configuration setting. The default query\_size setting is 100.
- **nt**  
Displays the Windows file attributes as well as the Privileged Access Manager properties.
- **props(all|propName [,propName ...])**  
Defines a new ruler for this class for this query and future queries.
- **unix**  
Displays the UNIX file attributes as well as the Privileged Access Manager properties.
- **useprops(propName [,propName ...])**  
Defines a ruler for this query only. The class ruler is unaffected.

### Example

The user root wants to list the properties of the file record /etc/passwd.

- User root has the ADMIN attribute.

```
showfile /etc/passwd
```

## show x grp Command Display Group Properties

### Valid in the AC environment

The show[x]grp command displays the settings of all the Privileged Access Manager properties of a group record. Optionally, the native environment properties are also shown.

#### NOTE

The showgrp command also exists in the native environment but operates differently there.

You can execute a show[x]grp command if at least one of the following conditions are true:

- You have at least one of the following attributes: ADMIN, AUDITOR, and OPERATOR.
- You have the GROUP-ADMIN or GROUP-AUDITOR attribute in each group to be listed, or each group to be listed is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group.
- You are assigned read authority in the access control list of the GROUP record in the ADMIN class.

This command has the following format:

```
{showgrp|sg} {groupName |groupName [,groupName...] } \
[addprops(propName[,propName ...])] \
[next] \
[props(all | propName[,propName ...])] \
[useprops(propName[,propName ...])] \
[nt|unix]
```

- **addprops(propName [,propName ...])**  
Defines properties to be added to the ruler for this query only.
- **groupName**  
Specifies the group whose properties you want to list.  
groupName can contain wildcard characters.  
On UNIX, to display the properties of a group whose name contains a special character or space, type an extra slash (/) before the group name.
- **next**  
Display parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the query\_size configuration setting. The default query\_size is 100.
- **nt**  
Shows the group's details from the local Windows system in addition to the properties in the database.
- **props(all|propName [,propName ...])**  
Defines the ruler for this class for this query and future queries.
- **useprops(propName [,propName ...])**  
Defines a ruler for this query only. The class ruler is unaffected.
- **unix**  
Shows the group's details from the local UNIX system in addition to the properties in the database.

### Examples

- The user root wants to display the properties of the security group.
  - The user root has the GROUP-ADMIN attribute in the security group.
- The user admin wants to display the properties of all enterprise groups.
  - The user admin has the ADMIN and AUDITOR attributes.

```
showgrp security
```

```
showxgrp *
```

The properties of all enterprise groups defined to Privileged Access Manager are listed.



## showres Command Display Resource Properties

### Valid in the AC environment

The showres command displays the properties of resources belonging to classes in the database. The properties are listed in alphabetical order. The following classes can be listed using the showres command: ACVAR, ADMIN, CATEGORY, CONNECT, FILE, GHOST, GSUDO, GTERMINAL, HOST, HOSTNET, HOSTNP, SECFILE, SECLABEL, SUDO, SURROGATE, TERMINAL, PROGRAM, PROCESS, TCP, UACC, and any user defined class. Privileged Access Manager processes each resource independently and displays information only for those resources for which you have sufficient authority.

#### NOTE

This command also exists in the native Windows environment but operates differently there.

showres also displays information about any programs that have become untrusted. The information includes:

- The reason that the program became untrusted.
- The UID of the last user to access the program (not necessarily the user who caused the program to become untrusted).
- The date and time that this user accessed the program.

You can execute a showres command if at least one of the following conditions is true:

- You have at least one of the following attributes: ADMIN, AUDITOR, and OPERATOR.
- You are the owner of the resource.
- You are assigned read authority in the access control list of the object representing the resource class record in the ADMIN class.

This command has the following format:

```
{showres|sr} classNameresourceName \

[addprops(propName [,propName...])] \

[next] \

[props(all | propName [,propName...])] \

[useprops(propName [,propName...])]
```

- **addprops(propName [,propName...])**  
Defines properties to be added to the current ruler for this query only.
- **className**  
Specifies the name of the class to which the resource belongs. To list the resource classes defined to Privileged Access Manager, use the find command.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the query\_size configuration setting. The query size default is set at 100.
- **props(all|propName [,propName ...])**  
Defines a new ruler for this class for this query and future queries.
- **resourceName**

Specifies the name of the resource record whose properties are to be listed. When listing the properties of more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma.

Privileged Access Manager processes each resource record independently. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.

*resourceName* can contain wildcard characters.

On UNIX, to display the properties of a single resource record whose name contains a special character or space, type an extra slash (/) before the resource name.

- `useprops(propName [,propName ...])`  
Defines a ruler for this query only. The class ruler is unaffected.

### Example: List record properties

In this example the user Admin1 wants to list the properties of the records whose names match the mask `ath*` in the `TERMINAL` class.

User Admin1 has the `ADMIN` and `AUDITOR` attributes.

```
showres TERMINAL ath*
```

### Example: List host attributes

In this example the user Admin1 lists the attributes of the local host in the `HNODE` class.

```
PAMSC> showres HNODE '__local__'
```

```
(localhost)
```

```
Data for HNODE '__local__'
```

```
-----
```

```
Owner           : LOCALHOST\Administrator (USER)
```

```
Create time     : 13-Oct-2010 11:12
```

```
Update time     : 13-Oct-2010 11:13
```

```
Updated by      : LOCALHOST\Administrator (USER)
```

```
Attributes      :
```

```
REGISTERED_NAME=localhost.domain.com
```

```
MAC_ADDRESS=00-50-56-B5-6B-XD
```

In this example, the command returns the following attributes:

- `REGISTERED_NAME=localhost.domain.com`
- `MAC_ADDRESS=00-50-56-B5-6B-XD`

## show x usr Command Display User Properties

### Valid in the AC environment

The show[x]usr command displays the values of all the properties of one or more users defined to Privileged Access Manager.

Use showusr to display the properties of internal users. Use showxusr to display the properties of enterprise users.

#### NOTE

The showusr command also exists in the native environment but operates differently there.

You can always list the properties of your own user record. To list properties of another user's record, one of the following conditions must be true:

- You are the owner of the user record.
- You have at least one of the following attributes: ADMIN, AUDITOR, and OPERATOR.
- The user record is within the scope of a group in which you have at least one of the following group attributes: ADMIN, AUDITOR, OPERATOR.
- You are assigned read authority in the access control list of the USER record in the ADMIN class.

This command has the following format:

```
{showusr|su |showxusr |sxu } [ {userName |(userName [,userName...]) } ] \
[addprops(propName [,propName...])] \
[next] \
[props( all | propName [,propName...])] \
[useprops(propName[,propName...])] \
[nt|unix]
```

- **addprops(propName [,propName...])**  
Defines properties to be added to the current ruler for this query only.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the query\_size configuration setting. The query size default is set at 100.
- **nt**  
Displays the user Windows' properties in addition to the properties in the database.
- **props(all|propName [,propName ...])**  
Defines a new ruler for this class for this query and future queries.
- **unix**  
Displays the user's UNIX properties in addition to the properties in the database.
- **userName**  
Defines the name of a user. It can include wildcard characters.  
On UNIX, to display the properties of a single user record whose name contains a special character or space, type an extra slash (/) before the group name.  
If you do not specify *userName*, the command displays the properties of your own user record.
- **useprops(propName [,propName ...])**  
Defines a ruler for this query only. The class ruler is unaffected.

### Examples

- The user root wants to list the properties of enterprise user Robin. The root has ADMIN and AUDITOR attributes.  
`showxusr Robin`
- The user root wants to list the user properties of enterprise users Robin and Leslie. The root has ADMIN and AUDITOR attributes.  
`showxusr (Robin,Leslie)`

## source Command Execute Commands from a File

### Valid in all environments

The source command allows you to execute one or more selang commands that have been placed in a file. Privileged Access Manager reads the specified file, executes the commands, and returns a selang prompt. Any user defined in the database can use this command.

This command is like the source command in csh and tcsh in UNIX.

This command has the following format:

```
source fileName
```

- **fileName**  
Specifies the name of the file that contains the selang commands.

### Example

The user admin wants to execute the commands in the file called initf1. The user enters the following command:

```
source initf1
```

## start dbexport Command Initiate Database Export

### Valid in the AC environment

The start dbexport command exports the Privileged Access Manager database of the host you are connected to, and copies the output to a buffer. If you are connected to a PMDB, you can also use this command to export the PMD database.

#### NOTE

Use the get dbexport command to view the output.

This command has the following format:

```
start dbexport [pmdname(name)] [filter("CLASS, CLASS...")] [param("depend=yes")] [param("edit=yes")]
```

- **filter("CLASS, CLASS...")**  
(Optional) Defines the classes to export from the database. If you do not specify a class, all rules in the database are exported.
- **param("depend=yes")**  
(Optional) Specifies to export dependent classes along with the class that you specify in the filter parameter. When you specify this parameter, Privileged Access Manager exports the specified class and the following dependent classes:

If you export rules that modify resources in a particular class, and the class has a corresponding resource group, Privileged Access Manager also exports the rules that modify resources in that resource group.

If you export rules that modify resources in a particular resource group, Privileged Access Manager also exports the rules that modify the member resource of the resource group.

If you export rules that modify resources in a particular class and that class has a PACL, Privileged Access Manager also exports the rules that modify resources in the PROGRAM class.

If you export rules that modify resources in a particular class and that class has a CALACL, Privileged Access Manager also exports the rules that modify resources in the CALENDAR class.

If you export rules that modify resources in a particular class, and one of the resources in that class is a member of a CONTAINER resource group, Privileged Access Manager exports the rules that modify resources in the CONTAINER class and the rules that modify the resources that are members of each CONTAINER resource group.

- **param("edit=yes")**  
(Optional) Specifies that Privileged Access Manager changes each rule that creates a new resource or accessor to a rule that modifies the resource or accessor.  
**Example:** If you specify this parameter Privileged Access Manager changes all newres rules to editres rules.
- **pmdname(*name*)**  
(Optional) Defines the name of the PMD database to export.

### Example: Initiate Database Export

The following example initiates the export of rules that modify FILE and GFILE class resources. The rules are exported from seosdb, the Privileged Access Manager database on the host you are connected to.

```
start dbexport filter("FILE, GFILE")
```

### Example: Initiate Database Export with Dependent Classes

The following example initiates the export of rules that modify FILE class resources and any classes that are dependent on FILE class resources, and changes each rule that creates a new resource or accessor to a rule that modifies the resource or accessor:

```
start dbexport filter("FILE") param("depend=yes edit=yes")
```

## start devcalc Command Initiate Policy Deviation Calculation

### Valid in the AC environment

The start devcalc command initiates policy deviation calculation and sends deviation status. The deviation data is stored in a local policy deviation data file (deviation.dat) and policy deviation status is sent to a DMS through one or more set DHs. To retrieve the actual deviation data, you need to run the get devcalc command.

#### NOTE

You do not need to run the deviation calculator manually. If you use advanced policy management, the policyfetcher does this for you regularly. If you have enterprise reporting enabled, the Report Agent also does this regularly. For more information about policy deviation calculation, see the *Enterprise Administration Guide*.

To run the start devcalc command you must have terminal access rights to the computer and execute access to DEVCALC sub-administration class.

This command has the following format:

```
start devcalc [params("-pn name#xx -strict -nonotify -precise")]
```

- **-nonotify**  
(Optional) Specifies that devcalc does *not* send deviation status to the DMS through the DH.

#### NOTE

The deviation calculation command policyfetcher runs is defined in the devcalc\_command configuration setting and, by default, uses this option to avoid sending deviation status twice.

- **-pn *name#xx***  
(Optional) Defines a comma-separated list of POLICY objects (policy version) the deviation calculator should calculate differences for. If no policy is specified, the deviation calculator calculates differences for all policies deployed on the local host.
- **-strict**  
(Optional) Compares between the policies associated with the local HNODE object and the ones associated with the HNODE object on the first available DMS.

Normally, the deviation calculator checks for deviations only on the local host. If this option is specified, the deviation calculator also compares the local policies to the policies on the first available DMS in the list. It compares the:

- a. List of policies associated with the HNODE object representing the local host.
- b. Policy state of each POLICY object associated with the HNODE object.
- c. Policy signature of each POLICY object associated with the HNODE object.

Use this option when you need to validate the result of the deviation calculation.

#### NOTE

If you have a large number of endpoints running the deviation calculation simultaneously, the DMS will be heavily loaded. We recommend that you configure your endpoints to use a DMS list or divide your hierarchy into smaller hierarchies and use this option within those smaller hierarchies.

- **-precise**

(Optional) Specifies that the deviation report also displays added objects, properties, and values that exist in the endpoint database and are not found in the policy. By default, the report only displays missing and mismatched items. Use this option when you would like to view the contents on the endpoint database and compare it to the deployed policy.

#### Example: Start a Policy Deviation Calculation for a Specific Policy

The following example shows how you can use the start devcalc command to calculate policy deviations for the second version of a policy called myPolicy and send the deviation status to the DMS list specified in the local Privileged Access Manager database:

```
PAMSC> start devcalc params("-pn myPolicy#02")
```

## start\_transaction Command Start Recording Dual Control Transactions

### Valid on UNIX hosts in the AC environment

The start\_transaction and end\_transaction commands create a file that contains an unprocessed transaction for Dual Control PMDB processes, with one or more commands. The administrator (any user with the ADMIN attribute) who entered the commands in the transaction is called a Maker. The commands must be authorized by a Checker (any administrator who is *not* the Maker) before they are executed in the PMDB.

The Checker must lock transactions before they can be processed. Until the transaction is locked by the Checker, the Maker can retrieve it, change the commands, or delete it. (See the sepmdb utility in the *Reference Guide* for details.) When the Maker enters the end\_transaction command, the transaction receives a unique id number. If the Maker wants to edit or retrieve the transaction later, this identifying number must be added after the transaction's name in the start\_transaction command. When the Maker retrieves the transaction, the name of the Maker, the id number of the transaction, and a short description are displayed (if the Maker entered a description in the *transactionName* parameter).

A Maker cannot change the transactions of other Makers. The objects used in a transaction cannot be used by other Makers in different transactions until the commands have been processed.

Each unprocessed transaction stays in a separate file until a Checker processes it. The Checker can authorize or reject a transaction. If the transaction is authorized, the commands are executed and the PMDB is changed accordingly. If the Checker rejects the transaction, the commands are deleted and the PMDB is not changed.

When the end\_transaction command is entered at the end of the Maker's work, the numeric id of the transaction appears. The commands can fail for the following reasons:

- if a command refers to an object that has been used in a different transaction which has not been processed yet
- if a command pertains to the Maker-you cannot change yourself
- if a command contains invalid syntax
- if a command refers to objects that do not exist (in this case a warning message appears)
- You can execute the start\_transaction and end\_transaction commands if you have the ADMIN attribute.
- Since the hosts command must be executed before invoking the start\_transaction and end\_transaction commands, you must be authorized to use the hosts command.

**Note:** For more information on Dual Control, see the *Endpoint Administration Guide for UNIX*.

#### Usage notes:

- The hosts command must be executed before invoking the start\_transaction and end\_transaction commands, and the name of the PMDB must be maker.
- In order for the start\_transaction and end\_transaction commands to function, the value for the is\_maker\_checker token in the pmd.ini file and in the [pmd] section of the seos.ini file must be set to yes.

This command has the following format:

```
start_transaction transactionName [transactionId]
.
.
.
end_transaction
```

- **transactionName**  
Specifies the name or a description of the transaction. You can enter a string of up to 256 alphanumeric characters.
- **transactionId**  
Specifies the unique number given to the transaction when it is created. This numeric id appears automatically when you create a transaction. You must specify this id number when you update the same transaction.

#### Examples

- The Maker Sally wants to add user Anne to the PMDB, and restrict their access to the system to weekdays between 8:00 a.m. and 8:00 p.m. Then Sally wants to change the default access to the tty30 terminal to read only. Sally wants to call this transaction general.

– The Maker has the ADMIN attribute.

```
hosts maker@
start_transaction general
newusr anne
(days (weekdays) time (0800:2000))
chres TERMINAL tty30
defaccess(read)
end_transaction
```

When Sally enters the end\_transaction command, the transaction is assigned an ID number, such as seven.

- The Maker Sally wants to add the FINANCIAL category to the user Anne. Sally added the user Anne record earlier the same day, and the command has not yet been processed or implemented on the PMDB.

– The Maker has the ADMIN attribute.

```
hosts maker@
start_transaction general 7
chusr anne category(FINANCIAL)
end_transaction
```

## unalias Command Remove selang Aliases

### Valid on UNIX hosts

The unalias command removes an alias defined by the alias command.

**Note:** You can list all defined aliases and their values using the alias command.

This command has the following format:

```
unalias aliasName
```

- *aliasName*  
Specifies the name of the alias you want to delete from the database.

## undeploy Command Initiate Policy Removal

### Valid in the AC environment

This command is a synonym of the deploy- command.

## selang Commands in the Remote Configuration Environment

This section contains a complete alphabetic reference to all the selang commands that operate on the Privileged Access Manager configuration resources (commands in the config environment).

## editres config Modify Configuration Settings

### Valid in the config environment

Use the editres config command to modify Privileged Access Manager configuration settings.

The editres config command has different formats for different sets of files. These sets are:

- Audit configuration files (audit.cfg and auditrouteflt.cfg) and PMDB filter files
- All other files

This command has the following syntax for audit configuration files and PMDB filter files:

```
editres config name [line+|- (value)] [clear]
```

This command has the following syntax for all other files:

```
editres config name section(path) token[-] (name) value[+|-] (value) data_type(type)
```

- *name*  
Specifies the configuration resource you want to modify. To modify a PMDB filter file, specify the file name in the format *pmdname@filter*, for example, *master\_pmdb@filter.flt*  
**Note:** For a list of configuration resources for the host you are managing, use the *find config* command.
- *clear*  
Deletes all values from the audit configuration file or PMDB filter file.

### NOTE

This option does not delete comments from the file.

- *data\_type(type)*  
Specifies the data type of the configuration entry.  
**Values:** str, numeric, multi\_str  
**Default:** str



**NOTE**

For UNIX, `data_type` can only be `str`. Other data types are not applicable to UNIX, as it stores configuration settings in files (text strings).

- `line+(value)`  
Defines the value you want to add to the audit configuration file or PMDB filter file.

**NOTE**

The *value* can be a value or a comment.

- `line-(value)`  
Defines the value you want to remove from the audit configuration file or PMDB filter file.

**NOTE**

The *value* can be a value or a comment.

- `section(path)`  
Defines the section of the configuration resource that you want to modify.

**NOTE**

For Windows registry settings, if you do not specify this option, the command modifies the registry key *name* defines.

- `token(name)`  
Defines the name of the configuration entry that you want to modify.
- `token-(name)`  
Defines the name of the configuration entry that you want to remove.
- `value(value)`  
Defines the value that you want to assign to a configuration entry. If a value for the configuration entry already exists, Privileged Access Manager replaces the value with *value*.  
If you do not specify a *value*, the command resets the configuration entry value.
- `value+(value)`  
(Windows REG\_MULTI\_SZ registry entries only) Defines the value that you want to append to a configuration entry.  
(All other configuration values) Defines the value that you want to assign to a configuration entry. If a value for the configuration entry already exists, Privileged Access Manager replaces the value with *value*.

**NOTE**

To ensure `selang` correctly translates the assigned value, enclose the value in quotes (" ").

- `value-(value)`  
(Windows REG\_MULTI\_SZ registry entries only) Defines the value that you want to remove from a configuration entry.  
(All other configuration values) Specifies to remove any value from the configuration entry.

**Examples: Modify ACROOT Configuration Settings on Windows**

The following examples show how to modify Privileged Access Manager for Windows configuration settings.

- This example configures Privileged Access Manager to use Audit Only mode:  

```
er CONFIG ACROOT section(SeOSD) token(GeneralInterceptionMode) value(1)
```
- This example adds a domain name to the list of domain names Privileged Access Manager maintains for host name resolution. The `domain_names` registry entry is a REG\_MULTI\_SZ registry entry:  

```
er CONFIG ACROOT section(SeOSD) token(domain_names) value+(company.com)
```
- This example removes a domain name from the list of domain names Privileged Access Manager maintains for host name resolution. The `domain_names` registry entry is a REG\_MULTI\_SZ registry entry:  

```
er CONFIG ACROOT section(SeOSD) token(domain_names) value-(company.com)
```
- This example removes a configuration setting:  

```
er CONFIG ACROOT section(AccessControl) token-(Emulate)
```
- This example configures the parent Policy Model of a Policy Model on the managed host:

```
er config myPMDb@PMDROOT token(Parent_Pmd) value(topPMDb@host1.comp.ca)
```

### Examples: Modify seos.ini Configuration Settings on UNIX

The following examples show how to modify Privileged Access Manager for UNIX configuration settings.

- This example configures Privileged Access Manager to enable PAM authentication:  

```
er CONFIG seos.ini section(seos) token(pam_enabled) value(yes)
```
- This example configures the domain name that Privileged Access Manager maintains for host name resolution:  

```
er CONFIG seos.ini section(seosd) token(domain_names) value+(company.com)
```
- This example removes the domain name that Privileged Access Manager maintains for host name resolution:  

```
er CONFIG seos.ini section(seosd) token(domain_names) value-(company.com)
```
- This example removes a configuration setting:  

```
er CONFIG seos.ini section(serevu) token-(admin_user)
```

### Example: Modify Audit Configuration File

The following example adds a line to the audit configuration file:

```
er CONFIG audit.cfg line+("FILE;*;Administrator;*;R;P")
```

### Example: Modify PMD Filter File

The following example adds a line to the PMD filter file:

```
er config pmdb@filter line+("*;*;USER;*;OLD_PASSWD;PASS")
```

## find config List Configuration Resources

### Valid in the config environment

The find config command lists the Privileged Access Manager configuration resources for the host you are managing. These resources can be registry keys or configuration files.

Possible resources vary by host type:

UNIX	Windows
seos.ini	ACROOT
pmd.ini@ <i>pmd_name</i>	pmd_name@PMDROOT
	SEOSDRV

This command has the following format:

```
find config
```

### NOTE

This command does not return a list of audit.cfg or auditrouteflt.cfg configuration files.

### Example: List Configuration Resources for a Windows Host

The following example shows the output of the find config command on a Windows host that has a Policy Model named pmdb:

```
PAMSC(config)> find config
```

```
(localhost)
```

```
pmdb@PMDROOT
```

```
ACROOT
```

```
SEOSDRV
```

## showres config Display Configuration Information

### Valid in the config environment

Use the showres config command to display Privileged Access Manager configuration information.

The showres config command has different formats for different sets of files. These sets are:

- Audit configuration files (audit.cfg and auditrouteflt.cfg) and PMDB filter files
- All other files

This command has the following syntax for audit configuration files and PMDB filter files:

```
showres config name
```

This command has the following syntax for all other files:

```
showres config name [section(path)] [token(name)] [recursive] [section_only]
```

- **name**  
Specifies the configuration resource you want to view information about. To view information about a PMDB filter file, specify the file name in the format *pmdbname@filter*, for example, master\_pmdb@filter.flit

#### NOTE

For a list of configuration resources for the host you are managing, use the *find config* command.

- **section(path)**  
(Optional) Defines the section of the configuration resource that you want to view information about. If you do not specify this option, the command lists all of the configuration entries and sections in the *name* configuration resource.
- **token(name)**  
(Optional) Defines the name of the configuration entry that you want to view information about. If you do not specify this option, the command lists all configuration entries and sections in the section(*path*) you defined.
- **recursive**  
Specifies to display information about all configuration entries and sections in all sub sections.
- **section\_only**  
Specifies to display information about sections only (no configuration entries will be listed).

## selang Commands in the Native UNIX Environment

This section contains a complete alphabetic reference to all the selang commands that operate on the UNIX system files (commands in the native UNIX environment).

**Use the table of contents to access the topics in this section.**

## chfile Command Modify UNIX File Settings

### Valid in the native UNIX environment

The chfile and editfile commands change the settings of one or more UNIX files.

#### NOTE

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{{chfile|cf}}{{editfile|ef}} fileName \
[owner(userName)] \
[group(groupName)] \
[mode( \[fowner(string)] \[fgroup(string)] \[fother(string)] \
)]
```

- **fileName**  
Specifies the name of the file whose settings are to be changed. Enter at least one UNIX file name. When changing more than one file, enclose the list of file names in parentheses and separate the file names with a space or a comma.
- **group(groupName)**  
Changes the group to which the file belongs. Specify a valid group name.
- **mode**  
Updates the access modes of the file.
- **fowner(string)**  
Specifies the access modes for the owner of the file. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Use the letter s to make a file setuid.  
Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If you do not specify a prefix, the previous permissions are reset to *string*.
- **fgroup(string)**  
Specifies the access modes for the file's group. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Use the letter s to make a file setgid.  
Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If you do not specify a prefix, the previous permissions are reset to *string*.
- **fother(string)**  
Specifies the access modes that apply to other accessors. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If no prefix is specified, the previous permissions are reset to *string*.
- **owner(userName)**  
Changes the owner of the file. Specify the user name of a valid UNIX user.

## chgrp Command Modify UNIX Groups

### Valid in the native UNIX environment

Use the chgrp, editgrp, and newgrp commands to work with UNIX groups. These commands are identical in structure and only vary in the following way:

- The chgrp command *modifies* one or more UNIX groups.
- The editgrp command *creates or modifies* one or more UNIX groups.
- The newgrp command *creates* one or more UNIX groups.

**NOTE**

Groups are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/group. For more information, see the *Endpoint Administration Guide for UNIX*.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{{chgrp|cg}}|{{editgrp|eg}}|{{newgrp|ng}} groupName \
[groupid(integer)] \
[userlist(userNames)]
```

- **groupid(integer)**  
Sets the group ID of the group. Enter a positive integer representing the group's unique numeric ID. Privileged Access Manager does not allow a group ID of zero.
- **groupName**  
Specifies the name of the group to be modified. Specify the name of an existing UNIX group. When altering more than one group, enclose the list of group names in parentheses and separate group names with a space or a comma.
- **userlist(userNames)**  
Specifies a new member list. Each user name must already be defined to UNIX. When more than one user is in the list, separate the user names with a space or comma. The user list specified here replaces any previous user list defined to the group.

## chusr Command Modify UNIX Users

### Valid in the native UNIX environment

Use the chusr, editusr, and newusr commands to work with UNIX users. These commands are identical in structure and vary only in the following ways:

- The chusr command *modifies* one or more UNIX users.
- The editusr command *creates or modifies* one or more UNIX users.
- The newusr command *creates* one or more UNIX users.

**NOTE**

Users are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/passwd. For more information, see the *Endpoint Administration Guide for UNIX*.

**NOTE**

This command also exists in the Privileged Access Manager environment but operates differently there.

This command has the following format:

```
{{chusr|cu}}|{{editusr|eu}}|{{newusr|nu}} userName \
[enable] \
[gecos(string)] \
[homedir({path|nohomedir})] \
[password(string)] \
[pgroup(groupName)] \
[shellprog(path)] \
[userid(number)]
```

- **enable**  
Enables the login of a user account that was disabled for any reason. This is a chusr and editusr parameter.
- **gecos(string)**

Specifies a string containing general comments about the user, such as the user's full name. Enclose the string in single quotation marks.

- **homedir(*path*|nohomedir)**  
Specifies the full path of the user's home directory. Privileged Access Manager attempts to create the directory. If the path you specify ends with a slash, *groupname* is concatenated to the specific path. The UNIX file is updated, regardless of whether Privileged Access Manager successfully creates the home directory.  
If you specify nohomedir, UNIX does not create a homedir for the user.
- **password(*string*)**  
Assigns a password to the user. Specify any character except a blank space. The password is valid for one login only. When the user next logs in to the system, a new password must be set.
- **pgroup(*groupName*)**  
Specifies the user's primary group name.
- **shellprog(*path*)**  
Specifies the full path of the initial program or shell that is executed after the user invokes the login command or the su command.
- **userid(*number*)**  
Specifies the user's unique numeric ID, used for unique discretionary access control. Enter a decimal number greater than 100; values less than 100 are not accepted.
- **userName**  
The name of an existing UNIX user. When changing more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.

## editfile Command Modify UNIX File Settings

### Valid in the native UNIX environment

This command is documented with the chfile command.

## editgrp Command Create and Modify UNIX Groups

### Valid in the native UNIX environment

This command is documented with the chgrp command.

## editusr Command Create and Modify UNIX Users

### Valid in the native UNIX environment

This command is documented with the chusr command.

## find file Command List Native Files

### Valid in the native environment

Use the find file command to list all the system files that match the mask, which is a string. The files are ordered chronologically in one column.

This command has the following format:

```
find file [directory] [/mask]
```

- *directory*  
Lists all the files in the directory *directory*.
- *mask*  
Lists all the files in the directory *directory* that match the *mask* variable. The *mask* may include wildcard characters.

### Example: Find Executable Program Files in a Specific Path on Windows

The following command lists all executable files in the Privileged Access Manager bin directory:

```
find file C:\Program\Files\CA\PAMSC\bin\*.exe
```

### Example: Find Files Matching a Pattern on UNIX

The following command lists all files in the Privileged Access Manager bin directory that begin with the letter se:

```
find file <installpath2>/bin/se*
```

## join Command Add Users to Native Groups

### Valid in the native environments

The join command adds users to a group. The specified users and group must already be defined to native OS.

#### NOTE

This command also exists in the AC environment but operates differently.

To use the join command, at least one of the following must be true:

- You have the ADMIN attribute in your Privileged Access Manager user record.
- The group record is within the scope of a group in which you have the GROUPADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

#### NOTE

Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify Privileged Access Manager GROUP records and native groups.

This command has the following format:

```
{join|j} userName group(groupName)
```

- *group(groupName)*  
Specifies the native group to which the users are being added.
- *userName*  
Specifies the user name of the native user who is being connected to the group specified by the group parameter. When specifying more than one user, enclose the user names in parentheses and separate the user names with a space or a comma.

### Example

The user Eli wants to join the user Bob to the group staff.

- Eli has the ADMIN attribute and the current environment is *native*.

```
join Bob group(staff)
```

## join- Command Remove Users from Native Groups

### Valid in the native environments

The join command removes users from a group.

#### NOTE

This command also exists in the AC environment but operates differently.

To use the join command, one of the following conditions must be true:

- You have the ADMIN attribute.
- The group record is within the scope of a group in which you have the GROUPADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

If you only have ownership of the user's profile, you do not have sufficient authority to remove the user from a group. Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify Privileged Access Manager records and native groups

This command has the following format:

```
{join
  |j
} userName group(groupName)
```

- **group(groupName)**  
Specifies the native group from which to remove the user.
- **userName**  
Specifies the user name of the user you want to remove from the group. When removing more than one user from the group, enclose the list of user names in parentheses and separate the user names with a space or a comma.

### Example

The user Bill wants to remove the users sales25 and sales43 from the PAYROLL group.

- The user Bill has the ADMIN attribute and the current environment is *native*.

```
join
(sales25 sales43) group(PAYROLL)
```

## newgrp Command Create UNIX Groups

### Valid in the native UNIX environment

This command is documented with the chgrp command.

## newusr Command Create UNIX Users

### Valid in the native UNIX environment

This command is documented with the chusr command.

## rmgrp Command Delete UNIX Groups

### Valid in the native UNIX environment

The rmgrp command deletes one or more groups from the UNIX system.



**NOTE**

This command also exists in the AC environment but operates differently.

**NOTE**

Groups are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/group. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{rmgrp|rg} groupName
```

- **groupName**  
Specifies the name of the group to be deleted. The group name must be an existing UNIX group name. Specify one or more group names. When removing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

## rmusr Command Delete UNIX User

### Valid in the native UNIX environment

The rmusr command removes one or more users from the UNIX system.

**NOTE**

This command also exists in the AC environment but operates differently.

**NOTE**

Users are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/passwd. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{rmusr|ru} userName
```

- **userName**  
Specifies the user name of an existing UNIX user. When removing more than one user, enclose the list of user names in parentheses and separate the user names with a space or a comma.

## showfile Command Display Native File Properties

### Valid in the native environments

The showfile command lists the native details of one or more system files.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{showfile|sf} fileName [next] \
[{{props|addprops} (propNames)}]
```

- **addprops(propName)**  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- **fileName**  
Specifies the name of the file whose details are to be listed. Enter one or more UNIX file names. When specifying more than one file, enclose the list of file names in parentheses and separate the individual names with a space or a comma.
- **next**

Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the `query_size` configuration setting. The query size default is set at 100.

- `props(all|propName)`  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.

### Example: Show the Details of a UNIX File

You want to list the details of the UNIX file `/tmp/foo`.

```
showfile /tmp/foo
```

### Example: Show the Owner of a Windows File

You want to know who the owner of the Windows file `C:\tmp\foo.exe` is.

```
showfile C:\tmp\foo.exe props (Owner)
```

## showgrp Command Display Native Group Properties

### Valid in the native environments

The `showgrp` command displays the details of one or more groups in the native operating system.

#### NOTE

This command also exists in the AC environment but operates differently.

#### NOTE

On UNIX, groups are read, added, updated, and deleted from the file specified in the configuration settings (`seos.ini`); by default, this file is `/etc/group`. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{showgrp|sg} groupName [next] \
[ {props|addprops} (propNames) ]
```

- `addprops(propName)`  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- `groupName`  
Specifies the name of the group whose details are to be displayed. The group name must be an existing native group name. Specify one or more group names. When listing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the `query_size` configuration setting. The query size default is set at 100.
- `props(all|propName)`  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.

### Example

To list details of the UNIX group *security* when you are in the *unix* environment, enter the following command:

```
showgrp security
```

## showusr Command Display Native User Properties

### Valid in the native UNIX environment

The showusr command displays the properties of one or more users defined in the native operating system.

#### NOTE

This command also exists in the AC environment but operates differently.

#### NOTE

On UNIX, users are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/passwd. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{showusr|su} userName [next] \
[{props|addprops} (propNames) ]
```

- **addprops(propName)**  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- **userName**  
Specifies the name of the user whose native properties are to be displayed. Specify an existing native user name. When listing the properties of more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the query\_size configuration setting. The query size default is set at 100.
- **props(all|propName)**  
Sets the properties (ruler) to be displayed. The ruler remains set for future queries.

### Example

To list details of the UNIX user *leslie* when you are in the *unix* environment, enter the following command:

```
showusr leslie
```

## selang Commands in the Native Windows Environment

This section contains a complete alphabetic reference to all the selang commands that operate on the native Windows environment.

**Use the table of contents to access the topics in this section.**

## authorize Command Set Accessors Authority to Access Windows Resources

### Valid in the native Windows environment

The authorize command maintains the lists of users and groups authorized to access a particular resource. Using authorize, you can change a list to:

- Permit access to a resource for specific Privileged Access Manager users or groups.
- Block access to a resource for specific Privileged Access Manager users or groups.
- Change the level of access authority to a resource for specific users or groups.

**NOTE**

This command also exists in the AC environment but operates differently.

The following Windows environment classes support ACLs, and can be controlled by the authorize command.

- COM
- DISK
- FILE
- PRINTER
- REGKEY
- SHARE

Classes that do not appear in the list have no access control lists and cannot be controlled by the authorize command.

This command has the following format:

```
{authorize|auth} classNameresourceName \
[access(accessValue)|deniedaccess(accessvalue)] \
[gid(groupName, ...)] \
[uid(userName, ...)]
```

- **access(*accessValue*)**  
Specifies the access authority you want the accessors you identify in the uid or gid parameters to have to the resource.
- **className**  
Specifies the name of the class to which *resourceName* belongs.
- **deniedaccess(*accessvalue*)**  
Specifies the negative access authority that you want accessors, who you identify in the uid or gid parameters, to have to the resource.  
The denied *accessvalue* can be: all, create, delete, join, modify, none, password, or read.

**NOTE**

You can only use *accessValue* with the authorize command, not with authorize-.

- **gid(*groupName*)**  
Specifies the Windows group or groups whose access authority to the resource you are setting. The value *groupName* represents the name of one or more Windows groups. When specifying more than one group, separate the group names with a space or a comma.
- **resourceName**  
The name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.  
Privileged Access Manager processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.
- **uid(*userName*)**  
Specifies the Windows users whose access authority to the resource you are setting. *userName* is the user name of one or more Windows users. When specifying more than one user, separate the user names with a space or a comma. To specify all users who are defined in Windows, specify an asterisk (\*) for *userName*.

## authorize- Command Remove Accessors' Authority to Access Windows Resources

### Valid in the native Windows environment

The authorize- command removes the access authority to a resource by deleting the accessors from the standard access control list. This leaves the default access to determine accessors' ability to access a particular resource.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{authorize|auth-} classNameresourceName \
[gid(groupName, ...)] \
[uid(userName, ...)]
```

- **className**  
Specifies the name of the class to which *resourceName* belongs.
- **gid(groupName)**  
Specifies the Windows group or groups whose access authority to the resource you are setting. The value *groupName* represents the name of one or more Windows groups. When specifying more than one group, separate the group names with a space or a comma.
- **resourceName**  
Specifies the name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.  
Privileged Access Manager processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.
- **uid(userName)**  
Specifies the Windows users whose access authority to the resource you are setting. *userName* is the user name of one or more Windows users. When specifying more than one user, separate the user names with a space or a comma. To specify all users who are defined in Windows, specify an asterisk (\*) for *userName*.

## chfile Command Modify Windows File Settings

### Valid in the native Windows environment

The chfile and editfile commands are identical. They modify one or more Windows files.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following format for NTFS file systems:

```
{{chfile|cf}}{{editfile|ef}} fileName \
[attrib(attributeValue)] \
[attrib(-attributeValue)] \
[defaccess(accessValue)] \
[owner(userName|groupName)]
```

This command has the following format for FAT file systems:

```
{{chfile|cf}}{{editfile|ef}} fileName \
[attrib([-]attributeValue)]
```

- **attrib([-]attributeValue)**  
Specifies a set of attributes that determine the character of the file. When a minus sign (-) precedes the argument *value*, this parameter removes the attribute.
- **defaccess(accessValue)**  
Specifies the access authority for the Native security built-in group Everyone. All the system users are members of the Everyone group. Providing access to the Everyone group covers all the potential anonymous users in addition to all authenticated users.

**NOTE**

Default access for an object defined in the Privileged Access Manager environment has a different meaning; the default access authority is the authority granted to any accessor who is not in the resource's Privileged Access Manager list who requests access to the resource. The default access also applies to users not defined in Privileged Access Manager.

The defaccess parameter applies only to NTFS file systems.

- **owner(*userName|groupName*)**  
Assigns a user or group as the owner of the file record. The owner of the file record has unrestricted access to the file. The owner of the file may always update or delete the file record.

## chgrp Command Modify Windows Groups

### Valid in the native Windows environment

Use the chgrp, editgrp, and newgrp commands to work with Windows groups. These commands are identical in structure and only vary in the following way:

- The chgrp command *modifies* one or more Windows groups.
- The editgrp command *creates or modifies* one or more Windows groups.
- The newgrp command *creates* one or more Windows groups.

**NOTE**

This command also exists in the AC environment but operates differently.

When defining more than one group or changing the properties of more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

**NOTE**

To add or remove members from a group use the join or join- command.

This command has the following format:

```
{{chgrp|cg}}{{editgrp|eg}}{{newgrp|ng}} groupName \
[global] \
[comment(string)|comment-] \
[privileges(privList)] \
[privileges(-privList)] \
[rename_group]
```

- **comment(*string*)**  
Adds an alphanumeric comment string of up to 255 characters to the group record. If you previously added a comment string to the group record, the new string specified here replaces the existing string. If the string contains any blanks, enclose the entire string in single quotation marks.  
Standard Windows groups have a descriptive comment added on system installation. If you create a new group in both the Windows and AC environments, Privileged Access Manager inserts the comment Privileged Access Manager Group.
- **global**  
Indicates a global group. Each group name must be unique and cannot currently exist in the Windows database. Windows does not allow groups and users to share the same name.

**NOTE**

Use *~groupName* when you create global groups and use the services of Privileged Access Manager version 4.1. Version 4.1 and above support this format for backward compatibility.

- *groupName*

**NOTE**

For the command `newgrp`, specifies the name of the group record added to the database. Each group name must be unique and must not currently exist in the Windows database. Unlike the Privileged Access Manager database, Windows does not allow groups and users to share the same name.

For the command `chgrp`, specifies the name of the group whose properties you are changing.

When defining more than one group or changing the properties of more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

- `privileges(privList[-privList])`

Adds specific rights to the Windows group record or, when `privList` is preceded by a minus sign (-), removes the specified rights. Valid values are any of the privileges available in native Windows.

You can specify this parameter only with the `chgrp` or `editgrp` command, and only when you are changing an existing group record. You cannot use it to assign privileges when you are creating a new group record.

- `rename_group`

Renames the group account in the Windows database. All the properties of the old group name apply to the renamed group account. Each group name must be unique and must exist in the Windows database. Unlike the Privileged Access Manager database, Windows does not allow groups and users to share the same name.

**NOTE**

When Privileged Access Manager is installed on Windows 2000 with Active Directory, it renames the pre-Windows 2000 group name.

## chres Command Modify Windows Resources

### Valid in the native Windows environment

Use the `chres`, `editres`, and `newres` commands to work with resource records that belong to a Privileged Access Manager class in the Windows environment. These commands are identical in structure and only vary in the following way:

- The `chres` command *modifies* one or more resources.
- The `editres` command *creates or modifies* one or more resources.
- The `newres` command *creates* one or more resources.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following formats:

```
{{chres|cr}}{{editres|er}}{{newres|nr}} classNameresourceName \
[comment(string)|comment-] \
[defaccess(accessValue)] \
[dword(integer)|string(string)|binary(hexastring)|multistring(string)] \
[location(string)|location()] \
[maxusers(integer)] \
[owner(userName|groupName)] \
[share_name(string)|sharename-]
```

or

```
{{chres|cr}}{{editres|er}}{{newres|nr}} \
DOMAIN resourceName \
[computer(workstationName)|computer-(workstationName)] \
[domainpwd(connectPassword)] \
[trusted(domainName)|trusted-(domainName)]
```

- `binary(hexastring)`

Specifies the value of a registry key when it is a hexadecimal.

- *className*  
Specifies the name of the class to which *resourceName* belongs.  
For the newres command, valid values are: REGKEY, REGVAL, OU, and SHARE. For the chres and editres commands, valid values are: COM, DISK, DOMAIN, FILE, PRINTER, REGKEY, REGVAL, SERVICE, DEVICE, SESSION, OU, and SHARE.
- *comment(string)*  
Adds a comment string to the resource record. If you previously added a comment string to the resource record, the new string specified here replaces the existing string. This parameter is valid for SHARE and PRINTER resources only.
- *computer(workstationName)|computer-(workstationName)*  
Specifies the name of the workstation you are adding to the domain, or, when a minus sign precedes the argument, the name of the workstation you are removing from the domain. This parameter can only be used with DOMAIN resources. You can specify this parameter only with the chres or editres command.
- *defaccess(accessValue)*  
Specifies the access authority for the Native security built-in group Everyone. All the system users are members of the Everyone group. Providing access to the Everyone group covers all the potential anonymous users in addition to all authenticated users.

#### NOTE

Defaccess for an object defined in the Privileged Access Manager environment has a different meaning; the default access authority is the authority granted to any accessor who is not in the resource's Privileged Access Manager list who requests access to the resource. The default access also applies to users not defined in Privileged Access Manager.

The defaccess parameter applies only to NTFS file systems.

- *domainpwd(connectPassword)*  
Specifies the password an administrator must enter when changing trust relationships.  
This parameter can only be used with DOMAIN resources. You can specify this parameter only with the chres or editres command.
- *dword(integer)*  
Specifies the value of a registry key when it is an integer.
- *gen\_prop(propertyName)*  
Specifies the property for the OU class.  
This parameter is valid for the OU class only.
- *gen\_value(valueName)*  
Specifies the property value for the OU class.  
This parameter is valid for the OU class only.
- *location(string)*  
Indicates the location of a printer. Use ( ) with blanks to remove this property.  
This parameter is valid for PRINTER resources only.
- *maxusers(integer)*  
Specifies the maximum number (*integer*) of users that can connect to a shared directory at one time.  
This parameter is valid for SHARE resources only.
- *multistring(string)*  
Specifies the value of a registry key when it is a multistring.
- *owner(userName|groupName)*  
Assigns a user or group as the owner of the resource record. The owner of the resource record has unrestricted access to the resource. The owner of the resource is always permitted to update and delete the resource record. For more information, see the *Endpoint Administration Guide for Windows*.  
For FILE or SHARE records on a FAT file system, you may not specify the owner parameter. This parameter is also not valid for DEVICE, DOMAIN, OU, PROCESS, REGVAL, SERVICE, and SESSION resources.
- *resourceName*



The name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.

Privileged Access Manager processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, Privileged Access Manager issues a message and continues processing with the next resource in the list.

- `share_name(shareName)|share_name-`  
Identifies the share point for a printer.  
This parameter is valid for PRINTER resources only.
- `string(string)`  
Specifies the value of a registry key when it is a string.
- `trusted(domainName) | trusted-(domainName)`  
Specifies the name of the domain you are adding to trusted domains, or, when a minus sign precedes the argument, the name of the domain you are untrusting. This parameter can only be used with DOMAIN resources. You can specify this parameter only with the `chres` or `editres` command.

## chusr Command Modify Windows Users

### Valid in the native Windows environment

Use the `chusr`, `editusr`, and `newusr` commands to work with Windows users. These commands are identical in structure and only vary in the following way:

- The `chusr` command *modifies* one or more Windows users.
- The `editusr` command *creates or modifies* one or more Windows users.
- The `newusr` command *creates* one or more Windows users.

### NOTE

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{ {chusr|cu} | {editusr|eu} | {newusr|nu} } userName \
[comment(string)|comment-] \
[country(string)] \
[expire|expire(mm/dd/yy[@hh:mm])|expire-] \
[flags( (accountFlags) |-(accountFlags) )] \
[full_name(fullName)] \
[homedir(homeDir)] \
[homedrive(homeDrive)] \
[location(string)] \
[logonserver(serverName)] \
[organization(name)] \
[org_unit(name)] \
[password(password)] \
[pgroup(primaryGroup)] \
[phone(string)] \
[privileges(privList)] \
[profile(path)] \
[restrictions( \days({[mon] [tue] [wed] [thu] [fri] [sat] [sun] }|anyday|weekdays) \time(startTime:endTime|
anytime))]\
[restrictions-] \
[resume[(date)]|resume-] \
[script(logonScriptPath)] \
```

```
[suspend[(date)] | suspend-] \
[terminals (terminalList) | terminals- (terminalList)] \
[workstations (workstationList) | workstations- (workstationList) | workstations-]
```

- **comment(*string*)|comment-**  
Assigns a comment string to the user record.  
The argument is an alphanumeric string of up to 255 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **country(*string*)**  
Specifies the country where the user is located. This string is not used during the authorization process.  
The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **expire|expire(*mm/dd/yy*[@*hh:mm*]) | expire-**  
Sets the date on which the user's account expires. If a date is not specified, the user account expires immediately, provided the user is not currently logged in. If the user is logged in, the account expires when the user logs out.  
expire- with the newusr command defines a user account that does not have an expiration date. For the chusr and editusr commands, it removes an expiration date from the specified user account.  
The date argument takes the format: *mm/dd/yy* [@*hh:mm*].
- **flags(*accountFlags*)|- *accountFlags*)**  
Specifies particular attributes of a user's account. See the appendix Windows Values for a list of valid flag values.  
To remove flags from the user record, precede *accountFlags* with a minus (-).
- **full\_name(*fullName*)**  
Specifies the full name of the user associated with the user record.  
The argument is an alphanumeric string of up to 256 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **gecos(*string*)**  
Specifies a comment string for the user, such as the user's full name. Enclose the string in single quotation marks.
- **homedir(*homeDir*)**  
Specifies the user's home directory. Users log in automatically to their own home drives and home directories.
- **homedrive(*homeDrive*)**  
Specifies the drive of the user's home directory. Users log in automatically to their own home drives and home directories.
- **location(*string*)**  
Specifies the user's location. This string is not used during the authorization process.  
The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **logonserver(*serverName*)**  
Specifies the server that verifies the login information for the user. When the user logs in to the domain workstation, Privileged Access Manager transfers the login information to the server, which gives the workstation permission for the user to work.
- **organization(*name*)**  
Specifies the organization in which the user works. This information is not used during the authorization process.  
The argument is an alphanumeric string of up to 256 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **org\_unit(*name*)**  
Specifies the organizational unit in which the user works. This information is not used during the authorization process.  
The argument is an alphanumeric string of up to 256 characters. If the string contains any blanks, enclose the entire string in single quotation marks.
- **password(*password*)**  
Assigns a password to a user. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, a new password must be set.

The argument is a string of up to 14 characters, and cannot include either a space or a comma. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, the user must set a new password, unless you set the flag for Password Never Expires.

To change your own password, you need to set `selang` options using `setoptions cng_ownpwd` or use `sepass`.

If you are setting passwords for users on Windows NT systems, the following message may appear:

The password is shorter than required.

This error means that the password does not meet the policy requirements. This is caused by any of the following:

- The password is shorter or longer than the required length.
- The password has been used recently and exists in the Windows NT Change History field.
- The password does not have enough unique characters.
- The password does not meet other password policy requirements (such as those set with Privileged Access Manager password policies).

To avoid this error, make sure you set a password which meets all applicable requirements.

- `pgroup(primaryGroup)`  
Sets the user's primary group ID. A primary group is one of the groups in which a user is defined and must be a Global group.  
The argument is a string of up to 14 characters, and cannot include either a space or a comma.
- `phone(string)`  
Specifies the user's phone number. This information is not used during the authorization process.
- `privileges(privList)`  
Adds specific rights to the Windows user record or, when `privList` is preceded by a minus sign (-), removes the specified rights. You can specify this parameter only with the `chusr` or `editusr` command, and only when you are changing an existing user record. You cannot use it to assign privileges when you are creating a new user record.
- `profile(path)`  
Specifies the full path location of the file that contains a user's profile for the Desktop environment (program groups, network connections). Every time the user logs in to any workstation, the same environment appears on the screen.
- `restrictions([days] [time])|restrictions-([days] [time])`  
Specifies the days of the week and the hours in the day when users may access the file.  
If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users may access the system only during the specified time period on the specified days.
  - [Days] specifies the days on which users may access the file. The days argument takes the following sub-arguments:
    - a. **anyday**-Allow users access to the file on any day.
  - **weekdays**-Allow users access to the resource only on weekdays-Monday through Friday.
    - a. **Mon, Tue, Wed, Thu, Fri, Sat, Sun**-Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
  - [Time] specifies the period during which users may access the resource. The time argument takes the following sub-arguments:
    - a. **anytime**-Allow users access to the resource at any time of the day.
    - b. **startTime:endTime**-Allow access to the resource only during the specified period. The format of both `startTime` and `endTime` is `hhmm`, where `hh` is the hour in 24-hour notation (00 through 23) and `mm` is the minutes (00 through 59). Note that 2400 is not a valid time value. `startTime` must be less than `endTime`, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time (1100:2000).
- `resume(date)|resume-`

The date, and optionally time, at which Windows will reinstate the user account. If you specify both the suspend parameter and the resume parameter, make sure the resume date falls after the suspend date or the user will stay suspended indefinitely.

Enter a date, and optional time, in the following format:

```
mm/dd/yy[@HH:MM]
```

Use resume- parameter to change the status of the user account from active (enabled) to suspended. Use this parameter with the chusr or editusr commands only.

- **script(*loginScriptPath*)**  
Specifies the location of a file that runs automatically when the user logs in. This login script configures the working environment. This parameter is optional, since the profile parameter also sets up the user's working environment.
- **suspend(*date*)|suspend-**  
Disables a user account. A user cannot use a suspended user account to log in to the system. If you specify date, Windows suspends the user account on the specified date. If you omit a date, Windows suspends the user account immediately upon execution of the chusr command.  
Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM]*.  
Use the suspend- parameter to change the status of the user account from disabled to active (enabled). Use this parameter with the chusr or editusr commands only.
- **terminals(*terminalList*)|terminals-(*terminalList*)**  
Specifies up to eight terminals from which the user can log in. Surround the list with quotation marks, and separate the names with commas. For example:  

```
"terminal1,terminal2"
```
- **workstations(*workstationList*)|workstations-(*workstationList*)|workstations-**  
Specifies up to eight workstations from which the user can log in. Surround the list with quotation marks, and separate the names with commas. For example:  

```
"workstation1,workstation2"
```

## editfile Command Modify Windows File Settings

### Valid in the native Windows environment

This command is documented with the chfile command.

## editgrp Command Create and Modify Windows Groups

### Valid in the native Windows environment

This command is documented with the chgrp command.

## editusr Command Create and Modify Windows Users

### Valid in the native Windows environment

This command is documented with the chusr command.

## editres Command Create and Modify Windows Resources

### Valid in the native Windows environment

This command is documented with the chres command.

## find file Command List Native Files (Windows)

### Valid in the native environment

Use the find file command to list all the system files that match the mask, which is a string. The files are ordered chronologically in one column.

This command has the following format:

```
find file [directory] [/mask]
```

- **directory**  
Lists all the files in the directory *directory*.
- **mask**  
Lists all the files in the directory *directory* that match the *mask* variable. The *mask* may include wildcard characters.

### Example: Find Executable Program Files in a Specific Path on Windows

The following command lists all executable files in the Privileged Access Manager bin directory:

```
find file C:\Program\Files\CA\PAMSC\bin\*.exe
```

### Example: Find Files Matching a Pattern on UNIX

The following command lists all files in the Privileged Access Manager bin directory that begin with the letter *se*:

```
find file /opt/CA/PAMSC/bin/se*
```

## find xuser xgroup Command List Enterprise Users or Groups

### Valid in the native Windows environment

The find {xuser|xgroup} command lists the names of enterprise users or groups in the current or *trusted* domains.

#### NOTE

This command is supported only on supported Windows 2000 operating systems with Directory Services.

This command has the following format:

```
find {xuser|xgroup} mask [domain(domainName)] [next]
```

- **xgroup**  
Specifies for the command to return enterprise groups.
- **xuser**  
Specifies for the command to return enterprise users.
- **domain(domainName)**  
Defines the trusted domain to restrict the search to.  
If you do not specify this option, the command returns users from the current domain.
- **mask**  
Defines a mask for the enterprise users.
- **next**

Specifies that selang output should continue the listing of enterprise users or groups that was started by a previous find xuser or find xgroup command.

Use this option if there are more than 100 items in the list.

### Example: Display Enterprise Users

The following command lists the first 100 enterprise users in the current domain that begin with abc:

```
find xuser abc*
```

## join Command Add Users to Native Groups (Windows)

### Valid in the native environments

The join command adds users to a group. The specified users and group must already be defined to native OS.

#### NOTE

This command also exists in the AC environment but operates differently.

To use the join command, at least one of the following must be true:

- You have the ADMIN attribute in your Privileged Access Manager user record.
- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

#### NOTE

Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify Privileged Access Manager GROUP records and native groups.

This command has the following format:

```
{join|j} userName group(groupName)
```

- **group(groupName)**  
Specifies the native group to which the users are being added.
- **userName**  
Specifies the user name of the native user who is being connected to the group specified by the group parameter. When specifying more than one user, enclose the user names in parentheses and separate the user names with a space or a comma.

### Example

The user Eli wants to join the user Bob to the group staff.

- Eli has the ADMIN attribute and the current environment is *native*.

```
join Bob group(staff)
```

## join- Command Remove Users from Native Groups (Windows)

### Valid in the native environments

The join- command removes users from a group.

#### NOTE

This command also exists in the AC environment but operates differently.

To use the join- command, one of the following conditions must be true:

- You have the ADMIN attribute.
- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

If you only have ownership of the user's profile, you do not have sufficient authority to remove the user from a group. Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify Privileged Access Manager records and native groups

This command has the following format:

```
{join-|j-} userName group(groupName)
```

- **group(*groupName*)**  
Specifies the native group from which to remove the user.
- **userName**  
Specifies the user name of the user you want to remove from the group. When removing more than one user from the group, enclose the list of user names in parentheses and separate the user names with a space or a comma.

### Example

The user Bill wants to remove the users sales25 and sales43 from the PAYROLL group.

- The user Bill has the ADMIN attribute and the current environment is *native*.

```
join- (sales25 sales43) group(PAYROLL)
```

## newgrp Command Create Windows Groups

### Valid in the native Windows environment

This command is documented with the chgrp command.

## newres Command Create Windows Resources

### Valid in the native Windows environment

This command is documented with the chres command.

## newusr Command Create Windows Users

### Valid in the native Windows environment

This command is documented with the chusr command.

## rmgrp Command Delete Windows Groups

### Valid in the native Windows environment

The rmgrp command deletes one or more groups from the Windows database.

#### NOTE

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{rmgrp|rg} groupName
```

- *groupName*  
Specifies the name of the group to be deleted. The group name must be an existing Windows group name. Specify one or more group names. When removing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

## rmres Command Delete a Windows Resource

The rmres command removes one or more resources from the Windows system database.

### NOTE

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{rmres|rr} classNameresourceName
```

- *className*  
Specifies the name of the class the resource belongs to.
- *resourceName*  
Specifies the name of an existing Windows resource of class *className*. When removing more than one resource, enclose the list of user names in parentheses and separate the names with a space or a comma.

## rmusr Command Delete a Windows User

### Valid in the native Windows environment

The rmusr command removes one or more users from the Windows system database.

### NOTE

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{rmusr|ru} userName
```

- *userName*  
Specifies the user name of an existing Windows user. When removing more than one user, enclose the list of user names in parentheses and separate the user names with a space or a comma.

## setoptions Command Set CA Privileged Access Manager Server Control Windows Options

The setoptions command dynamically sets system-wide Privileged Access Manager options related to the Windows operating system.

### NOTE

This command also exists in the AC environment, but operates differently there.

You need ADMIN attribute to use the setoptions command, with the exception that you need only AUDITOR or OPERATOR attribute to use the command setoptions list.

This command has the following format:

```
setoptions|so \
[audit_policy( \
[success(system|logon|access|rights \ |process|security|manage)] \[failure(system|logon|access|rights \ |
process|security|manage)] \
```



```

    ])
    [password([history(number-stored-passwords)][interval(nDays)][min_life(NDays)]
    )]

```

[audit\_policy( \

```

    [success(system|logon|access|rights \
    |process|security|manage)] \
    [failure(system|logon|access|rights \
    |process|security|manage)] \

```

- **audit\_policy{+|-}**  
Specifies whether auditing is enabled (+) or disabled (-).
- **audit\_policy(success(system|logon|access|rights|process|security|manage))**  
Specifies which detected authorized access events are logged. The types of access are:
  - **system**-attempts to shutdown or restart the computer.
  - **logon**-attempts to log on to or log off from the system.
  - **access**-attempts to access securable objects, such as files.
  - **rights**-attempts to use Windows Server privileges.
  - **process**-events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
  - **security**-attempts to change Policy object rules.
  - **manage**-attempts to create, delete, or change user or group accounts. Also, password changes.
- **audit\_policy(failure(system|logon|access|rights|process|security|manage))**  
Specifies which detected unauthorized access events are logged. The types of access are:
  - **system**-attempts to shutdown or restart the computer.
  - **logon**-attempts to log on to or log off from the system.
  - **access**-attempts to access securable objects, such as files.
  - **rights**-attempts to use Windows Server privileges.
  - **process**-events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
  - **security**-attempts to change Policy object rules.
  - **manage**-attempts to create, delete, or change user or group accounts. Also, password changes.
- **history(number-stored-passwords)**  
Specifies the number of previous passwords that are stored in the database. When supplying a new password, the user cannot specify any of the passwords stored in the history list. *NStoredPasswords* is an integer between 1 and 24. If you specify zero, no passwords are saved.
- **interval(nDays)**  
Sets the number of days that must pass after passwords are set or changed before the system prompts users for a new password.  
The value of *nDays* must be a positive integer or zero. An interval of zero disables password interval checking for users. Set the interval to zero if you do not want passwords to expire.
- **min\_life(NDays)**  
Sets the minimum number of days between password changes. *NDays* must be a positive integer.

## showfile Command Display Native File Properties (Windows)

### Valid in the native environments

The showfile command lists the native details of one or more system files.

**NOTE**

This command also exists in the AC environment but operates differently.

This command has the following format:

```
{showfile|sf} fileName [next] \
[{props|addprops} (propNames)]
```

- **addprops(propName)**  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- **fileName**  
Specifies the name of the file whose details are to be listed. Enter one or more UNIX file names. When specifying more than one file, enclose the list of file names in parentheses and separate the individual names with a space or a comma.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the query\_size configuration setting. The query size default is set at 100.
- **props(all|propName)**  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.

**Example: Show the Details of a UNIX File**

You want to list the details of the UNIX file /tmp/foo.

```
showfile /tmp/foo
```

**Example: Show the Owner of a Windows File**

You want to know who the owner of the Windows file C:\tmp\foo.exe is.

```
showfile C:\tmp\foo.exe props (Owner)
```

**showgrp Command Display Native Group Properties (Windows)****Valid in the native environments**

The showgrp command displays the details of one or more groups in the native operating system.

**NOTE**

This command also exists in the AC environment but operates differently.

**NOTE**

On UNIX, groups are read, added, updated, and deleted from the file specified in the configuration settings (seos.ini); by default, this file is /etc/group. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{showgrp|sg} groupName [next] \
[{props|addprops} (propNames)]
```

- **addprops(propName)**  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- **groupName**

Specifies the name of the group whose details are to be displayed. The group name must be an existing native group name. Specify one or more group names. When listing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the `query_size` configuration setting. The query size default is set at 100.
- `props(all|propName)`  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.

### Example

To list details of the UNIX group *security* when you are in the *unix* environment, enter the following command:

```
showgrp security
```

## showres Command Display Native Resource Properties (Windows)

Displays the properties of Windows resources.

This command has the following format:

```
showres|sr classNameresourceName [next] \
[ {props|addprops} (propNames) ]
```

- `addprops(propName)`  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- `className`  
Specifies the name of the class the resource belongs to.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the `query_size` configuration setting. The query size default is set at 100.
- `props(all|propName)`  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.
- `resourceName`  
Specifies the name of an existing Windows resource of class *className*.

## showusr Command Display Native User Properties (Windows)

### Valid in the native UNIX environment

The `showusr` command displays the properties of one or more users defined in the native operating system.

#### NOTE

This command also exists in the AC environment but operates differently.

#### NOTE

On UNIX, users are read, added, updated, and deleted from the file specified in the configuration settings (`seos.ini`); by default, this file is `/etc/passwd`. For more information, see the *Endpoint Administration Guide for UNIX*.

This command has the following format:

```
{showusr|su} userName [next] \
```

```
[ {props|addprops} (propNames) ]
```

- **addprops(*propName*)**  
Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.
- **userName**  
Specifies the name of the user whose native properties are to be displayed. Specify an existing native user name. When listing the properties of more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.
- **next**  
Displays parts of the requested data. This option is useful when the query data is larger than the set query size. The maximum query size is determined by the `query_size` configuration setting. The query size default is set at 100.
- **props(all|*propName*)**  
Sets the properties (ruler) to be displayed.  
The ruler remains set for future queries.

### Example

To list details of the UNIX user *leslie* when you are in the *unix* environment, enter the following command:

```
showusr leslie
```

### xaudit Command Modify System Access Control List

The `xaudit` command adds entries in the system access control list (SACL). Each entry in this list causes an audit message to be logged when a specified user or group attempts to gain access to the resource. The `xaudit-` command removes entries from the SACL, and is valid for resource types FILE, PRINTER, REGKEY, DISK, COM, or SHARE.

This command has the following format:

```
xaudit classNameresourceName \  
[failure(auditMode)] \  
[gid(groupName)] \  
[success(auditMode)] \  
[uid(userName)]
```

- **className**  
Specifies the name of the resource type to which the resource belongs.
- **failure(*auditMode*)**  
Logs unauthorized access attempts to the resource.  
Valid values for *auditmode* depend on the resource type to which it belongs:

#### NOTE

Only NTFS files can have audit modes

- **DISK** and **COM**: changePermissions, delete, modify, query, read, synchronize, takeOwnership.
- **FILE**: changePermissions, delete, execute, read, takeOwnership, and write.
- **PRINTER**: changePermissions, delete, print, and takeOwnership.
- **REGKEY**: delete, enumerate, link, notify, queryValue, readControl, setValue, subkey, and write.

For all resource types: *none* and *all*.

- **gid(*groupName*)**  
Specifies the groups whose access to the resource is being audited. When specifying more than one group, separate the names with spaces or commas.
- **resourceName**

Specifies the name of the resource record whose system access control list (SACL) is being modified.

- **success(*auditMode*)**

Logs authorized accesses to the resource.

Valid values for *auditmode* depend on the resource type to which it belongs:

#### NOTE

Only NTFS files can have audit modes

- **DISK** and **COM**: changePermissions, delete, modify, query, read, synchronize, takeownership.
- **FILE**: changePermissions, delete, execute, read, takeOwnership, and write.
- **PRINTER**: changePermissions, delete, print, and takeOwnership.
- **REGKEY**: delete, enumerate, link, notify, queryValue, readControl, setValue, subkey, and write.

For all resource types: *none* and *all*.

- **uid(*userName*)**

Specifies the user whose access to the resource is being audited. When specifying more than one user, separate the user names with spaces or commas. To specify all users who are defined in the Windows NT database, specify an asterisk (\*) for *userName*.

## xaudit- Command Remove System Access Control List

The xaudit- command removes entries from the SACL, and is valid for resource types FILE, PRINTER, REGKEY, DISK, COM, or SHARE.

This command has the following format:

```
xaudit-className, resourceName \
    [gid(groupName)] \
    [uid(userName)]
```

- **className**  
Specifies the name of the resource type to which the resource belongs.
- **gid(*groupName*)**  
Specifies the groups or groups whose access to the resource is being audited. When specifying more than one group, separate the names with spaces or commas.
- **resourceName**  
Specifies the name of the resource record whose system access control list (SACL) is being removed.
- **uid(*userName*)**  
Specifies the user whose access to the resource is being audited. When specifying more than one user, separate the user names with spaces or commas. To specify all users who are defined in the Windows NT database, specify an asterisk (\*) for *userName*.

## PAM SC selang Commands in the Policy Model Environment

This section contains a complete alphabetic reference to all the selang commands that operate on the Policy Model environment.

**Use the table of contents to access the topics in this section.**

### backuppmd Command Back up a PMDB

#### Valid in the pmd environment

The backuppmd command backs up the data in the PMDB database to a specified directory. All the data in the PMDB database is backed up, including policies, deployment information, and configuration files.

This command has the following format for DMSs:

```
backup pmdName destination(path)
```

This command has the following format for PMDBs:

```
backup pmdName [destination(path)|hir_host(name)]
```

- **destination(*path*)**  
Defines the directory that you want the backup files to be stored in.

**NOTE**

If you do not specify a path, the files will be backed up to the default location specified in the `_pmd_backup_directory_` token. Default: (UNIX) `ACInstallDir/data/policies_backup/pmdName`

Default: (Windows) `ACInstallDir\data\policies_backup\pmdName`

- **pmdName**  
Defines the name of the PMDB or DMS to back up.
- **hir\_host(*name*)**  
Backs up all the PMDBs in a hierarchy to the host *name* that you specify, and modifies the PMDB subscribers so that the subscription still works when the backup is moved to the *name* host.

**NOTE**

This command is only supported if the master and child PMDBs are deployed on the same host.

## createpmd Command Create a PMDB on a Host

### Valid in the pmd environment

The `createpmd` command defines a PMDB on a remote host. You can designate one or more users as administrator, auditor, and password managers for the PMDB. You can also define the PMDB's parent and subscriber PMDBs. You can run `createpmd` command from a remote host.

This command has the following format:

```
createpmd pmdname \
[admins(user [user ...])] \
[auditors(user [user ...])] \
[pwman(user [user ...])] \
[parentpmd(pmdname@host)] \
[desktop(host-names...)] \
[subscriber(host-names|pmdnames...)] \
[pwdfile(file-name)] \
[grpfile(file-name)] \
[nis] \
[xadmins(user [user ...])] \
[xauditors(user [user ...])] \
```

- **admins(*user [user ...]*)**  
Specifies one or more internal users to be PMDB administrators. Separate multiple users with spaces.
- **auditors(*user [user ...]*)**  
Specifies one or more internal users who can view the audit file of the PMDB. Separate multiple users with spaces.
- **pwmans(*user [user ...]*)**  
Specifies one or more users as PMDB password managers. Separate multiple users with spaces.
- **parentpmd(*pmdname@host*)**  
Specifies the name of the PMDB that is a parent to the one you are creating.

**NOTE**

If you want to define multiple parent Policy Models with a `selang` remote command, you must to use quotation marks. For example, to create a Policy Model and define its parent, use the following command:

```
createpmd subs2 admins(abc123 root) auditors(abc123 root) desktop(pcp36949) \
parentpmd("aa@pcp36949,bb@pcp36949")
```

- **desktop(*host [host ...]*)**  
Specifies one or more hosts from which administrators can administer the PMDB. Separate multiple hosts with spaces. The default is the host of the new PMDB.
- **subscribers(*host | pmd [host | pmd ...]*)**  
Specifies the hosts or PMDBs to be a subscriber of the new PMDB. Separate multiple hosts or pmds with spaces.
- **pwdfile(*filename*)**  
Specifies the PMDB password file.
- **grpfile(*filename*)**  
Specifies the PMDB group file.
- **nis**  
Performs an NIS setup on the new PMDB's host, and creates a filter file to filter out all UNIX updates.
- **xadmins(*user [user ...]*)**  
Specifies one or more enterprise users to be PMDB administrators. Separate multiple users with spaces.
- **xauditors(*user [user ...]*)**  
Specifies one or more enterprise users who can view the audit file of the PMDB. Separate multiple users with spaces.
- **pwmans(*user [user ...]*)**  
Specifies one or more enterprise users as PMDB password managers. Separate multiple users with spaces.

**deletepmd Command Remove a PMDB from a Host****Valid in the pmd environment**

The `deletepmd` command removes the following items from the host:

- The PMDB's `selang` protection files:
  - database files
  - registry entries
- The contents of the PMDB directory
- The PMDB directory

**WARNING**

To prevent serious operational problems, avoid removing the PMDB by manually deleting its files. Always use the `deletepmd` command for PMDBs.

This command has the following format:

```
deletepmd pmdname
```

**findpmd Command List PMDBs on the Host****Valid in the pmd environment**

The `findpmd` command lists the PMDBs in the host to which you are connected and whether their daemons are loaded.

This command has the following format:

```
findpmd
```

## listpmd Command List Information about a PMDB

### Valid in the pmd environment

The listpmd command lists information about the PMDB and its subscribers, update file, and error log. If no options are used, the command lists all subscribers of the Policy Model *pmdName*.

This command has the following format:

```
listpmd pmdName \
[info|subscriber(subNames)|cmd(offset) \
|errors|all_errors|log] \
[next]
```

- **cmd(offset)**

Displays all commands in the update file and their offsets.

The offset indicates the location of the update inside the file. If an offset is specified, the list starts from offset. If no offset is specified, the display begins from the beginning of the update file.

#### NOTE

The update file contains updates that must be, or have been, propagated by the PMDB. The offset indicates the location of the next update that must be sent to a subscriber. The update file's initial and latest offsets are displayed.

- **errors|all\_errors**

Displays the Policy Model error log. The *errors* parameter displays all types of errors except non-connection failure errors. *all\_errors* displays all errors.

- **info**

Displays general information about the Policy Model *pmdName*, including whether the Policy Model has a parent.

- **next** Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query\_size configuration setting located in the,

- (UNIX) [lang] section of the seos.ini file

- (Windows) lang subkey, as follows:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang

The query size default is set at 100.

- **pmdname**

Defines the name of the PMDB you want to list information for.

- **subscriber(subNames)**

Lists the subscribers of the Policy Model and their status, including number of errors, availability, offset, and the next command to be propagated. The *subNames* parameter lets you select a subset of subscribers.

- **log**

Displays the policy model general log file.

### Example: Display PMDB subscriber information for selected subscribers

To display a list of subscribers to the myPMDB Policy Model that begin with the letters *compInt*, enter the following command:

```
listpmd myPMDB subscriber(compInt*)
```

## pmd Command Control a PMDB

### Valid in the pmd environment

The pmd command clears the Policy Model error log, updates the subscriber list, starts and stops the Policy Model service, and truncates the update file.



This command has the following format:

```
pmd pmdName \
{[release(subname)|start|stop|truncate(offset)|lock|unlock \
|reloadini|startlog|killog|clrerror|backup|operation]}
```

- **backup**  
Moves the Policy Model to backup status.
- **clrerror|clrerr**  
Clears the Policy Model error log.
- **killog**  
Disables the Policy Model general log file. If you specify this option, no messages are written to the log.

#### **WARNING**

Do not use the kill command to shut down the PMDB service.

- **lock**  
Moves the Policy Model to lock status, and stops the Policy Model sending updates to its subscribers.
- **operation**  
Moves the Policy Model from backup to operational status.
- **pmdname**  
Defines the name of the PMDB that you want to execute the selected option on.
- **release(subName)**  
Removes the subscriber specified by *subName* from the list of unavailable subscribers. This means that the subscriber can receive updates immediately. *subName* specifies the subscriber that is to become available for update.
- **reloadini**  
(UNIX only) Rereads the policy model pmd.ini file and the seos.ini file, letting you change configuration settings without having to reload the policy model daemon.
- **startlog**  
Enables the Policy Model general log file for writing. Use this option if the log file has been disabled.
- **start**  
Starts the Privileged Access Manager Policy Model service. Use this option when there are no other commands to execute.
- **stop**  
Stops the Privileged Access Manager Policy Model daemon/service.
- **truncate|trunc[(offset)]**  
Deletes entries from the update file. If an offset is not specified, the file is truncated at the highest possible offset. The highest possible offset is the location of last command that successfully updated the subscriber. If *offset* is specified, all the entries up to the specified offset are deleted.

#### **NOTE**

You must now use the true offset provided by the *listpmd* command to truncate the file, and not an offset derived by subtracting from the start offset.

- **unlock**  
Moves the Policy Model from lock to unlock status, and lets the Policy Model send updates to its subscribers.

## **restorepmd Command Restore a PMDB**

### **Valid in the pmd environment**

The *restorepmd* command restores a PMDB on a local host. The backup files that you use to restore the PMDB must be from a host running the same platform, operating system, and version of Privileged Access Manager as the restoration host. Privileged Access Manager must be running on the restoration host.

**NOTE**

If you back up and restore the PMDB on different terminals, the PMDB does not automatically update the terminal resource in the restored PMDB database. You must add the new terminal resource to the restored PMDB. To add the new terminal resource, stop the restored PMDB, run the *selang -p pmdb* command, then start the restored PMDB.

This command has the following format:

```
restorepmd pmdName [source(path)] [admin(user)] [xadmin(user)] [parentpmd(name)]
```

- **admin(user)**  
(UNIX) Defines internal users as administrators of the restored PMDB.
- **pmdName**  
Defines the name of the PMDB to restore.
- **parentpmd(name)**  
(Optional) Defines the name of the restored PMDB's parent. Specify the name in the format *pmd@host*.
- **source(path)**  
(Optional) Defines the directory where the backup files are located. If you do not specify the source directory, the PMDB is restored from the files in the default location. The default location is defined in the *\_pmd\_backup\_directory\_* token.

**NOTE**

**Default:** (UNIX) *ACInstallDir/data/policies\_backup/pmdNameDefault*: (Windows) *ACInstallDir\data\policies\_backup\pmdName*

- **xadmin(user)**  
(UNIX) Defines enterprise users as administrators of the restored PMDB.

## subs Command Add Subscribers or Subscribe Databases

### Valid in the pmd environment

The subs command adds a subscriber to a parent PMDB or subscribes a database to a parent PMDB.

When you subscribe a host to a PMDB:

- The host must be up.
- Privileged Access Manager must be running on the host.
- The PMDB must be the parent PMDB of the subscribed host.

When you subscribe a PMDB to another PMDB:

- Privileged Access Manager must be running on the host in which the subscribed PMDB resides.
- Configure *parent\_pmd* as the parent of the subscribing PMDB.

**NOTE**

You can add a subscriber to a parent PMDB that resides on the same host only.

This command has the following format:

```
subs pmdname \  
[subs(subsname)] \  
[host_type(mfHost) sysid(sysID) mf_admin(mfAdmin) port(port)] \  
{offset(offset) }
```

or

```
subs pmdname [newsups(subsname)]
```

or

```
subs pmdname [parentpmd(pmdname2@host)]
```

- **host\_type(mfhost)**  
Specifies the mainframe host type of the subscriber.
- **mf\_admin(mfAdmin)**  
Specifies the mainframe administrator of the subscriber.
- **newsubs(subsname)**  
Subscribes *subsname* to policy model *pmdname*, and sends PMDB, password, and group files to the subscriber.
- **parentpmd(pmdName2@host)**  
Specifies the PMDB *pmdName2@host* the parent Policy Model of *pmdName*.
- **pmdname** Specifies the name of the PMDB you want to execute the selected option on.
- **port(port)**  
Specifies the port number of the subscriber.
- **subs(subsname)**  
Assigns a subscriber to the PMDB.
- **sysid(sysId)**  
Specifies the system ID of the subscriber.

## subspmd Command Change Parent PMDB

### Valid in the pmd environment

The subspmd command changes the parent of the Privileged Access Manager database in the host to which you are connected.

This command has the following format:

```
subspmd parentpmd(pmdname@host)
```

- **parentpmd(pmdname@host)**  
Makes *pmdname@host* the current host's parent policy model.

## unsubs Command Remove a Subscriber

### Valid in the pmd environment

The unsubs command removes a subscriber from the subscriber list of the Policy Model.

This command has the following format:

```
unsubs pmdName subs(subName)
```

- **pmdname**  
Defines the name of the PMDB you want to execute the selected option on.
- **subs(subName)**  
Defines the name of the subscriber you want to remove from the *pmdname* subscriber list.

## Classes and Properties

This section contains a description of each property in every class defined in the Privileged Access Manager database and in the native operating systems. Arranged in environments alphabetically by class, the chapter provides information on which properties you can modify, which selang parameters you use to update these properties, and which commands contain these parameters.

## Class and Property Information

The following conventions apply to the provided class and property information:

- In the descriptive material before the property lists, the *key* of the class record is defined. The key is the record identifier, which you specify when you create a new record. Once created, it becomes a non-modifiable property.
- The symbol [-] used with a parameter indicates that the parameter may be deleted from the database by typing it with a minus sign.  
For example, *comment* (with appropriate text) adds a comment to a database record; *comment-* removes the comment from the database. You cannot use parameters with a minus sign when creating a record.
- The two types of classes in the database are accessor classes and resource classes.  
You operate on records in the accessor classes (USER and GROUP) with different *selang* command sets than you use for the resource classes:
  - Use *chusr*, *editusr*, and *newusr* to operate on USER class records.
  - Use *chgrp*, *editgrp*, and *newgrp* to operate on GROUP class records.
  - Use *chres*, *editres*, and *newres* to operate on records in any of the resource classes. If the resource is a file, you may also use the *chfile* or *editfile* commands.
  - Use *showgrp*, *showres*, *showfile*, or *showusr* to list the properties of a record.
  - Use *authorize* and *authorize-* to add, change, or remove ACLs for resource records.

## Classes in the AC Environment

This section contains a complete alphabetic reference to all the classes and properties that exist in the Privileged Access Manager database (classes in the AC environment).

### ACVAR Class

Each record in the ACPVAR class defines a variable that is deployed on an endpoint. You cannot deactivate this class.

The key of the ACPVAR class is the name of the variable.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using *selang* or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **OWNER**  
Defines the user or group that owns the record.
- **POLICIES**  
(Informational) The list of policies (POLICY objects) that use this variable.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **VARIABLE\_TYPE**

Defines the variable type. Valid values are:

- **built-in**  
Specifies that the variable was created by Privileged Access Manager during installation. Static variables resolve based on the system settings of the endpoint.  
**Note:** You cannot modify or delete built-in variables.
- **osvar**  
Specifies that the variable resolves based on an operating system value.
- **regval**  
(Windows) Specifies that the variable resolves based on a registry value.  
**Note:** You can only define registry values that point to REG\_SZ or REG\_EXPAND\_SZ registry types.
- **static**  
Specifies that the variable resolves to the string value you define.

#### NOTE

You cannot change the variable type of an existing variable.

- **VARIABLE\_VALUE**  
Defines the values of the variable.  
**Note:** This property does not expand any nested variables within the variable value.
- **VARIABLE\_EXPANDED\_VALUE**  
(Informational) Defines the variable values and expands any nested variables within the variable values.

#### Examples:

To define a new static variable, specify:

```
nr ACVAR ACHOME type(static) value+("/opt/CA/PAMSC")
```

To define a new variable that is based on the system environment, specify:

```
nr ACVAR ACHOME type(OSVAR) value+(AC_HOME)
```

To add value to a variable, specify:

```
er ACVAR ACHOME value+("/opt/CA/PAMSC")
```

To remove value from a variable, specify:

```
er ACVAR ACHOME value-("/opt/CA/PAMSC")
```

## ADMIN Class

Each record in the ADMIN class contains definitions that allow non-ADMIN users to administer specific classes. You create an ADMIN record to represent each Privileged Access Manager class that delegated users administer. The record contains a list of accessors with the access authorities of each, and also supports Conditional Access Control Lists (CACLS). The key of the ADMIN class record is the name of the class being protected.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using Selang or the administration interfaces. Non-modifiable properties are marked as *informational*.

- **AAUDIT**(Informational) Displays the type of activity that Privileged Access Manager audits.
- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors access types. Each element in the Access Control List (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **CALACL**  
Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the Unicenter NSM calendar status.  
Each element in the calendar access control list (CALACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Calendar**  
Defines a reference to a calendar in Unicenter TNG.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Access is permitted only when the calendar is ON. Access is denied in all other cases.  
Use the calendar parameter with the authorize command to permit user or group access to the resource according to the access defined in the calendar ACL.
- **CALENDAR**  
Represents a Unicenter TNG calendar object for user, group, and resource restrictions. Privileged Access Manager fetches Unicenter TNG active calendars at specified time intervals.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **NACL**  
The *NACL* property of a resource is an access control list that defines accessors with authorization denied to a resource, together with the type of access that they are denied (example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the type of access that is denied to the accessor.  
Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.
- **NOTIFY**  
Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters

- **OWNER**

Defines the user or group that owns the record.

- **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program Access Control List (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `Selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests

- **success**

Granted access requests

- **failure**

Denied access requests (default)

- **none**

No access requests

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the `label[-]` parameter of the

`chres`

and

`ch[x]usr`

commands.

- **SECLEVEL** Defines the security level of an accessor or resource.

**NOTE**

This property corresponds to the `level[-]` parameter of the

`ch[x]usr`

and

`chres`

commands.

- **UACC**

Defines the default access authority for the resource, which indicates the access that is granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **WARNING**  
Specifies whether Warning mode is enabled. If the Warning mode is enabled on a resource, then access requests to the resource are granted. If an access request violates an access rule, then a record is written to the audit log.

**Example:** This example shows how to assign "Password Change" privileges to a user "John" by using the ADMIN class in UNIX/Linux endpoint.

**Step 1:** Create a user "John".

```
PAMSC> eu John password(John_Pwd)
```

**Step 2:** Use the ADMIN class to authorize "John" with the administrative privileges to change the password of any other user. The user can be any other user (including Admin user) but not the superuser (example, root).

```
PAMSC> authorize ADMIN USER uid(John) access(password)
```

**Step 3:** View all the Admin users with administrative privileges.

```
PAMSC> showres ADMIN USER
(localhost)
Data for ADMIN 'USER'
-----
Defaccess : None
ACLs :
Accessor Access
John (USER ) PW
Peter (USER ) R, Modify, Cre, Del, Join
Audit mode : Failure
Update time : 16-Feb-2017 15:06
Updated by : root (USER )
```

**Step 4:** John tries to perform operations such as create a user (Louis), view other users in the database but fails as he is not authorize to do so.

```
PAMSC> nu Louis

(localhost)
ERROR: Operation not allowed

PAMSC> su *
```



```
(localhost)
ERROR: Operation not allowed
```

**Step 5:** John tries to modify the password of another Admin user (Peter) and succeeds as he is authorized to do so.

```
PAMSC> eu Peter password(Peter_Pwd)
(localhost)
Successfully updated USER Peter
(localhost)
Native:
===
Successfully updated USER Peter
```

## AGENT\_TYPE Class

Each record in the AGENT\_TYPE class defines an agent type used by CA SSO.

The key of the AGENT\_TYPE class record is the type of the agent.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked as *informational*.

- **AGENT\_FLAG**  
Contains information about the attribute. The flag can contain the following values:
  - **aznchk**-Indicates whether to use this attribute for authorization.
  - **predef** (predefined), **freetext** (free text), or **userdir** (user directory)-Specify the source of the user attributes.
  - **user** or **group**-These values indicate whether the attribute (accessor) is a user or a group.
- **AGENT\_LIST**  
A list of objects in the AGENT class that were created with this AGENT\_TYPE object as the value for the agent\_type parameter; for example, this property is updated implicitly when creating an object in the AGENT class.
- **CLASSES**  
A multi-string list of the classes or resources that are relevant to this agent.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **OWNER**  
Defines the user or group that owns the record.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## APPL Class

Each record in the APPL class defines an application used by CA SSO.

The key of the APPL class record is the name of the application.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked as *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **APPLTYPE**  
Used by CA SSO.
- **AZNACL**  
Defines the authorization ACL. The authorization ACL is an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. Typically, when an AZNACL is used, the object is not in the database.
- **CAPTION**  
The text under the application's icon on the desktop. The default is the name of the APPL record.  
**Limit:** 47 alphanumeric characters.
- **CMDLINE**  
The file name of the application executable. Used by CA SSO.  
**Limit:** 255 characters.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CONTAINED\_ITEMS**  
The record names of the contained applications, if the record is a container.  
Use the `item[-](appName)` parameter with the `chres`, `editres`, and `newres` commands to modify this property.
- **CONTAINERS**  
The record names of container applications, if the record is contained in other applications.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **DIALOG\_FILE**  
The name of the CA SSO script in the directory containing the login sequence for the application. The default directory location is `/usr/sso/scripts`. The default value is no script.  
Use the `script[-](fileName)` parameter with the `chres`, `editres`, and `newres` commands to modify this property.
- **GROUPS**  
A list of user groups authorized to use the application.
- **HOST**  
The name of the host where the application resides.

Use the `host[-](hostName)` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **ICONFILE**

The file name or full path of the file containing the icon representing the application on the desktop. Privileged Access Manager expects to find the icon on the end user's workstation. If just a file name is entered, the search order for the file is as follows:

- a. Current directory
- b. Directories listed in the `PATH` environment variable

The default is the default icon of the workstation.

- **ICONID**

The numeric ID (if necessary) of the icon within the icon file. If the `ICONID` is not specified, the default icon is used.

- **IS\_CONTAINER**

Whether the application is a container. The default is no.

Use the `container[-]` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **IS\_DISABLED**

Whether the application is disabled. If the application is disabled, users cannot log into it. This feature is useful when you change an application and you do not want any users to log in to the application while you make it. The disabled application appears in the application menu list, but if a user selects the application the login is terminated with an appropriate message. The default is not disabled.

- **IS\_HIDDEN**

Whether the application icon appears on the desktop even for users who can invoke it. You may want to hide a *master* application, for example an application that only serves the purpose of supplying passwords to other applications. The default is not hidden.

Use the `hidden[-]` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **IS\_SENSITIVE**

Whether re-authentication is required when the user opens the application after a preset time. The default is not sensitive.

Use the `sensitive[-]` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **LOGIN\_TYPE**

The way user passwords are provided. The value is *pwd* (plain password), *otp* (One Time Password), *appticket* (a proprietary ticket for mainframe application authentication), *none* (no password required), or *passticket* (a one-time password replacement format created by IBM and used by mainframe security packages). The default is *pwd*.

Use the `login_type(value)` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **MASTER\_APPL**

The record name of the application that supplies the password to other applications. The default is no master.

Use the `master[-](appName)` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also *ACL*, *CALACL*, *PACL*. Each entry in the *NACL* contains the following information:

#### Accessor

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

#### NOTIFY

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## **OWNER**

Defines the user or group that owns the record.

## **PGMDIR**

A directory, or a list of directories, where the application's executable file resides. Used by CA SSO.

## **PWD\_AUTOGEN**

Indicates whether the application password is automatically generated by CA SSO. The default is no.

## **PWD\_SYNC**

Indicates whether the application password is automatically kept identical to those of the other applications. The default is no.

## **PWPOLICY**

The record name of the password policy for the application. A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. The default is no validity check.

## **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## **SCRIPT\_POSTCMD**

Indicates whether to execute one or more commands after the login script.

## **SCRIPT\_PRECMD**

Indicates whether to execute one or more commands before the login script.

## **SCRIPT\_VARS**

Used by CA SSO, a variables list with the variable values of the application script that are saved per application.

## **TKTKEY**

Used by CA SSO only.

## **TKTPROFILE**

Used by CA SSO only.

## **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

### WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## AUTHHOST Class

Each record in the AUTHHOST class defines an authentication host in CA SSO.

The key of the AUTHHOST class record is the name of the authorization host.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked as *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **AZNACL**  
Defines the authorization ACL. The authorization ACL is an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. Typically, when an AZNACL is used, the object is not in the database.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **ETHINFO**  
Ethernet information for a host.
- **GROUPS**  
The list of GAUTHHOST or CONTAINER records a resource record belongs to.

To modify this property in an AUTHHOST class record, you must change the MEMBERS property in the appropriate CONTAINER or GAUTHHOST record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **KEY**  
Used by CA SSO only.
- **NACL**

The **NACL** property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **OWNER**

Defines the user or group that owns the record.

#### **PATH**

Used by CA SSO only.

#### **PROPERTIES**

In UNIX dbdump only

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

#### **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

**SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

**SEED**

Used by CA SSO only.

**SERNUM**

The serial number of the authentication host.

**UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

**UNTRUST**

Defines whether the resource is untrusted or trusted. If the UNTRUST property is set, accessors cannot use the resource. If the UNTRUST property is not set, the other properties listed in the database for the resource are used to determine accessor's access authority. If a trusted resource is changed in any way, Privileged Access Manager automatically sets the UNTRUST property.

Use the trust[-] parameter with the chres, editres, or newres command to modify this property.

**UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

**UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

**USER\_DIR\_PROP**

(Informational). The name of the user's directory.

**USER\_FORMAT**

Used by CA SSO only.

**USERALIAS**

Contains all the user's aliases that are defined to a specific authhost.

**WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**CATEGORY Class**

Each record in the CATEGORY class defines a security category in the database.

The key of the CATEGORY class record is the name of the security category.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **OWNER**

Defines the user or group that owns the record.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## CONNECT Class

Each record in the CONNECT class defines a remote host that can use TCP over IPv4 or IPv6 to connect to that host from the local host.

### NOTE

If the CONNECT class is being used as a criterion for access, the TCP class cannot effectively control access. Use either the TCP class or the CONNECT class to protect a connection, not both.

The key of the CONNECT class record is the name of the remote host.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors access types.

Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the authorize or authorize- command to modify the ACL.

- **CALACL**

Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the Unicenter NSM calendar status.

Each element in the calendar access control list (CALACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Calendar**

Defines a reference to a calendar in Unicenter TNG.

- **Access**

Defines the access authority that the accessor has to the resource.

Access is permitted only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the access defined in the calendar ACL.

- **CALENDAR**

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in Privileged Access Manager. Privileged Access Manager fetches Unicenter TNG active calendars at specified time intervals.

- **CATEGORY**



Defines one or more security categories that are assigned to a user or a resource.

- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **NACL**  
The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also *ACL*, *CALACL*, *PACL*. Each entry in the *NACL* contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the type of access that is denied to the accessor.  
Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.
- **NOTIFY**  
Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.  
**Limit:** 30 characters.
- **OWNER**  
Defines the user or group that owns the record.
- **PACL**  
Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (*PACL*) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
  - **Access**  
Defines the access authority that the accessor has to the resource.

#### NOTE

You can use wildcard characters to specify the resource in a *PACL*.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a *PACL*. You can use the `authorize-` command to remove accessors from a *PACL*.

- **RAUDIT**  
Defines the types of access events that Privileged Access Manager records in the audit log. *RAUDIT* derives its name from Resource *AUDIT*. Valid values are:
  - **all**  
All access requests.
  - **success**

Granted access requests.

- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

- **UACC**

Defines the default access authority for the resource, which indicates the access that is granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example:** Control outgoing connections from Privileged Access Manager endpoint to a remote host.

**Step 1:** Add a remote host ([My\\_Remote\\_Host.example.com](#)) in /etc/hosts. Run the following command at the command prompt.

```
vi /etc/hosts
```

**Step 2:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildla -h
```

**Step 3:** Run the following command at the command prompt to verify that the remote host ([My\\_Remote\\_Host.example.com](#)) is added to /etc/hosts.

```
./sebuildla -H
```

**Step 4:** Define a rule that prevents Telnet connections from Privileged Access Manager endpoint to the specified remote host, by a specific user.

```
PAMSC> authorize CONNECT My\_Remote\_Host.ca.com uid(john) access(none)
```

To deny all user access to the remote host, use '\*' for uid.

```
PAMSC> authorize CONNECT My_Remote_Host.ca.com uid(*) access(none)
```

You can also specify a program on the remote host that a user is allowed to connect to.

```
PAMSC> authorize CONNECT My_Remote_Host.ca.com uid(john) via(pgm(/usr/bin/telnet))  
access(r)
```

**Step 5:** Log in as John user and try to connect to the remote host using Telnet. The connection fails but other connections are not affected.

## CONTAINER Class

Each record in the CONTAINER class defines a group of objects from other resource classes, thus simplifying the job of defining access rules when a rule applies to several different classes of objects. Members of a CONTAINER class record can be objects from any of the following classes:

- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DICTIONARY
- DOMAIN (Windows only)
- FILE
- GAPPL
- GAUTHHOST
- GFILE
- GHOST
- GSUDO
- GTERMINAL
- HNODE
- HOLIDAY
- HOST
- HOSTNET
- HOSTNP
- MFTERMINAL
- PARAM\_DESC
- POLICY
- PROCESS
- PROGRAM
- REGKEY (Windows only)
- RULESET
- SUDO
- SURROGATE
- TCP
- TERMINAL
- WEBSERVICE

**NOTE**

CONTAINER records can be nested in other CONTAINER records.

Before you specify an object as a member of a CONTAINER record, you must create a record for it in its appropriate class.

If an object in the container does not have an ACL in its appropriate class record, it inherits the ACL for the CONTAINER record of which it is a member.

The key of the CONTAINER class is the name of the CONTAINER record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Access**  
Defines the access authority that the accessor has to the resource.

Use the access parameter with the authorize or authorize- command to modify the ACL.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **MEMBERS**

The list of objects from any class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **OWNER**

Defines the user or group that owns the record.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the via(*pgm*) parameter with the selang authorize command to add programs, accessors, and their access types to a PACL. You can use the authorize- command to remove accessors from a PACL.

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## DEPLOYMENT Class

Each record in the DEPLOYMENT class defines a deployment or undeployment task for an endpoint. A deployment task includes information that the endpoint needs to deploy or undeploy a policy as required.

The key of the DEPLOYMENT class is the name of the deployment task, which is usually generated automatically.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **DMS\_NAME**

Defines the name of the DMS where the deployment task was created.

- **GPOLICY**  
Defines the name of the policy this deployment task was created for.
- **GROUPS**  
Defines the deployment package (GDEPLOYMENT) this deployment task is a member of.
- **HNODE**  
Defines the host this deployment task was created for.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **OPERATION**

Specifies the type of operation that the endpoint should perform as a result of this deployment task. Can be one of: Deploy, Undeploy.

#### **OWNER**

Defines the user or group that owns the record.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

#### **POLICY\_VERSION**

Defines the policy version this deployment task was created for.

#### **RESULT\_MESSAGE**

Defines the output from the deployment or undeployment selang script. These are the messages selang outputs when the policy deployment or undeployment scripts are run.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from *Resource AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## STATUS

Defines the status of the deployment task. Can be one of:

- **Success**Policy deployed without errors.
- **Warning**Deployment script executed with errors.
- **Fail**There was an error executing the deployment task.
- **No Action**The deployment package is effectively empty so there is nothing to do.

### NOTE

This can also be a result of the policy already being assigned to the host through a different deployment path.

- **Not Executed**Policy verification found one or more errors in the policy.
- **Out of Sync**The policy contains a variable and the variable value has changed on the endpoint.
- **Pending Deployment**The policy contains an undefined or unresolved variable.
- **Pending Prerequisite**The deployment task will be executed only after all prerequisite policies are deployed.
- **Pending Dependents**The deployment task will be executed (undeploy policy) only after all dependent policies are also undeployed.
- **Fix**The deployment task is waiting to be deployed again.

## TARGETTYPE

Defines the type of host (target) to limit the policyfetcher to process only Privileged Access Manager deployment packages. Can be one of: UNAB, AC, None.

## UACC



Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

### WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## DICTIONARY Class

Each record in the **DICTIONARY** class defines a word in a common dictionary stored in the Privileged Access Manager database to compare passwords to. When users change their passwords, the passwords are checked against each record in this **DICTIONARY** class.

In addition to adding records (words) to the **DICTIONARY** class, you can import dictionary words from external files by running a utility or program.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **OWNER**

Defines the user or group that owns the record.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. **RAUDIT** derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## DOMAIN Class

### Valid on Windows

Each record in the DOMAIN class defines a domain in the Windows network.

The key to the DOMAIN record is the domain name.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.  
Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

### Accessor

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

### NOTIFY

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## OWNER

Defines the user or group that owns the record.

## PACL

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### NOTE

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the `label[-]` parameter of the `chres` and `ch[x]usr` commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

**UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

**UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

**WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**FILE Class**

Each record in the FILE class defines the access that is allowed to a specific file or directory, or to files that match a file name pattern. You can define a rule even though a file is not yet created.

Device files and symbolic links can be protected like any other file. However, by protecting a link, you do not automatically protect the file that the link points to.

**NOTE**

On the NTFS file system, a record in the FILE class also defines the access to the file streams.

When you define a script as a file, allow both *read* and *execute* access to the file. When you define a binary, *execute* access is sufficient.

For users outside the *special\_restricted* group, the *\_default* record in the FILE class (if *\_default* record does not exist then the record for FILE in the UACC class) *protects only files that are part of Privileged Access Manager* such as the seos.ini, seosd.trace, seos.audit, and seos.error files. These files are not explicitly defined to *Privileged Access Manager*, but are automatically protected by *Privileged Access Manager*.

**NOTE**

*Privileged Access Manager* uses the PROGRAM class and not the FILE class to protect

```
setuid
and
setgid
programs.
```

The key of the FILE class record is the name of the file or directory protected by the record. The full path must be specified.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using Selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessor access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Access**  
Defines the access authority that the accessor has to the resource. Use the Access parameter with the authorize or authorize- command to modify the ACL.

- **CALACL**

Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the Unicenter NSM calendar status. Each element in the Calendar Access Control List (CALACL) contains the following information:

- **Accessor**

- Defines an accessor.
- **Calendar**  
Defines a reference to a calendar in Unicenter TNG. Use the Calendar parameter with the authorize command to permit user or group access to the resource according to the access defined in the calendar ACL.
- **Access**  
Defines the access authority that the accessor has to the resource. Access is permitted only when the calendar is ON. Access is denied in all other cases.
- **CALENDAR**  
Represents a Unicenter TNG calendar object for user, group, and resource restrictions in *Privileged Access Manager*. *Privileged Access Manager* fetches Unicenter TNG active calendars at specified time intervals.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. *Privileged Access Manager* does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property. The resolution of daytime restrictions is one minute.
- **Groups**  
The list of GFILE or CONTAINER records a resource record belongs to.  
**DB property:** GROUPS  
To modify this property in a FILE class record, change the MEMBERS property in the appropriate CONTAINER or GFILE record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres`, or `newres` command to modify this property.
- **NACL**  
The NACL property of a resource is an access control list. The list defines the accessors that are denied authorization to a resource, along with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the type of access that is denied to the accessor. Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.
- **NOTIFY**  
Defines the user to be notified when a resource or user generates an audit event. *Privileged Access Manager* can email the audit record to the specified user.  
**Limit:** 30 characters.
- **OWNER**  
Defines the user or group that owns the record.
- **PACL**  
Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `Selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

- **RAUDIT**

Defines the types of access events that *Privileged Access Manager* records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests

- **success**

Granted access requests

- **failure**

Denied access requests (default).

- **none**

No access requests

*Privileged Access Manager* records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member. Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the `label[-]` parameter of the

`chres`

and

`ch[x]usr`

commands.

- **SECLEVEL**

Defines the security level of an accessor or resource. This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.

- **UACC**

Defines the default access authority for the resource, which indicates the access that is granted to accessors who are not defined to *Privileged Access Manager* or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UNTRUST**

Defines whether the resource is untrusted or trusted. If the UNTRUST property is set, accessors cannot use the resource. If the UNTRUST property is not set, the other properties that are listed in the database for the resource are used to determine accessor access authority. If a trusted resource is changed in any way, *Privileged Access Manager* automatically sets the UNTRUST property.

Use the `trust[-]` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. If you enable the Warning mode on a resource, then all the access request to a resource is granted. If an access request violates an access rule, a record is written to the audit log.

**Example:** This example shows how to restrict user access to a file by using the FILE class in Unix/Linux endpoint.

**Step 1:** Create a file "/home/my\_home/hello.c".

```
PAMSC> nf /home/my_home/hello.c
```

**Step 2:** When a file is created, by default every one has read access. We create a policy that restricts default user access to the file "/home/my\_home/hello.c". This policy restricts even the superuser (example, root) from accessing the file.

```
PAMSC> er FILE("/home/my_home/hello.c") audit(all) owner(nobody) defaccess(none)
```

**Step 3:** View the file "/home/my\_home/hello.c" details.

```
PAMSC> sr FILE /home/my_home/hello.c
(localhost)
Data for FILE '/home/my_home/hello.c'
-----
Defaccess : None
Audit mode : All
Owner : nobody (USER )
Create time : 13-Feb-2017 14:58
Update time : 13-Feb-2017 15:04
Updated by : root (USER )
```

**Step 4:** A user logs in to the host and tries to access the file "/home/my\_home/hello.c". The policy restricts user from accessing the file.

```
Host_Machine_Name> ls -l /home/my_home/hello.c
/bin/ls: cannot access /home/my_home/hello.c: Permission denied
```

**Step 5:** Create a policy that authorizes superuser (root) to access this file.

```
PAMSC> AUTHORIZE FILE("/home/my_home/hello.c") uid(root) access(a)
```

**Step 6:** View the file "/home/my\_home/hello.c" details.

```
PAMSC> sr file /home/my_home/hello.c
(localhost)
Data for FILE '/home/my_home/hello.c'
-----
Defaccess : None
ACLs :
```

```

Accessor Access
root (USER ) R, W, X, Cre, Del, Chown, Chmod, Utime, Sec, Rename, Chdir
Audit mode : All
Owner : nobody (USER )
Create time : 13-Feb-2017 14:58
Update time : 16-Feb-2017 17:54
Updated by : root (USER )

```

## GAPPL Class

Each record in the GAPPL class defines a group of applications used by CA SSO. You must create an APPL class record for each application before adding it to a GAPPL record. You must then explicitly connect records of the APPL class to the GAPPL record in order to group them.

The key of the GAPPL class record is the name of the GAPPL record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.
- **AZNACL**  
Defines the authorization ACL. The authorization ACL is an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. Typically, when an AZNACL is used, the object is not in the database.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **GROUPS**  
The list of CONTAINER records a resource record belongs to.  
To modify this property in a GAPPL class record, you must change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **MEMBERS**  
The list of objects from the APPL class that are members of the group.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres`, and `newres` commands to modify this property.
- **NACL**

The **NACL** property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also **ACL**, **CALACL**, **PACL**. Each entry in the **NACL** contains the following information:

### Accessor



Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

## OWNER

Defines the user or group that owns the record.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## GAUTHHOST Class

Each record in the GAUTHHOST class defines a group of authentication hosts used by CA SSO. You must create an AUTHHOST class record for each application before adding it to a GAUTHHOST record. You must then explicitly connect records of the AUTHHOST class to the GAUTHHOST record in order to group them.

The key of the GAUTHHOST class record is the name of the GAUTHHOST record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **AZNACL**

Defines the authorization ACL. The authorization ACL is an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. Typically, when an AZNACL is used, the object is not in the database.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **GROUPS**

The list of CONTAINER records a resource record belongs to.

To modify this property in a GAUTHHOST class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **MEMBERS**

The list of objects from the AUTHHOST class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **OWNER**

Defines the user or group that owns the record.

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from *Resource AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

#### **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## GFILE Class

Each record in the GFILE class defines the access allowed to a group of specific files, specific directories, or files that match a name pattern. You must create a FILE class record for each application before adding it to a GFILE record. You must then explicitly connect records of the FILE class to the GFILE record in order to group them. A file need not have been created yet in order to have a FILE class record defined for it.

The key of the GFILE class record is the name of the GFILE record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **MEMBERS**  
The list of objects from the FILE class that are members of the group.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres`, and `newres` commands to modify this property.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

### Accessor

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

## NOTIFY

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## OWNER

Defines the user or group that owns the record.

## PACL

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### NOTE

You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the *selang authorize* command to add programs, accessors, and their access types to a PACL. You can use the *authorize-* command to remove accessors from a PACL.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the *audit* parameter of the *chres* and *chfile* commands to modify the audit mode.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## GDEPLOYMENT Class

Each record in the GDEPLOYMENT class defines a deployment package. A deployment package is created automatically on the DMS. The package groups together all the deployment tasks that are created as a result of the same transaction

(policy assignment, upgrade, and so on) and for a particular host. This means that each transaction you make creates the required number of deployment tasks (DEPLOYMENT objects) and groups these by host (GDEPLOYMENT objects).

The key of the GDEPLOYMENT class is the name of the deployment package, which is generated automatically.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Nonmodifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the access types of the accessors.

Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GHNODE**

Defines the host group this deployment package was created for.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **HNODE**

Defines the host this deployment package was created for.

- **MEMBERS**

The list of objects from the DEPLOYMENT class that are members of the group.

Use the `mem+` or `mem-` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource. The list also specifies the type of access that they are denied. Example: `write`. See also *ACL*, *CALACL*, *PACL*. Each entry in the NACL contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## OWNER

Defines the user or group that owns the record.

## PACL

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### NOTE

You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the *selang authorize* command to add programs, accessors, and their access types to a PACL. You can use the *authorize-* command to remove accessors from a PACL.

## POLICY

Defines the policy this deployment package was created for.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the *label[-]* parameter of the *chres* and *ch[x]usr* commands.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests
- **success**  
Granted access requests
- **failure**  
Denied access requests (default)
- **none**  
No access requests

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource. The product also does not record whether the access rules were applied to a group or class that had the resource as a member.

Use the *audit* parameter of the *chres* and *chfile* commands to modify the audit mode.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## TRIGGER

Specifies the reason this deployment package was created:

- Assign - A result of assigning a policy to a host, or a host to a host group.
- AutoAssign - A result of the DMS automatically assigning a host to a host group.
- UnAssign - A result of unassigning a policy from a host, or a host from a host group.
- Direct Deploy - A result of a direct deploy action.
- Direct Undeploy - A result of a direct undeploy action.
- Upgrade - A result of an upgrade action.
- Restore - A result of a restore action on a host (HNODE).
- Hnode Deletion - A result of deleting a host (HNODE).
- Ghnode Deletion - A result of deleting a host group (GHNODE).
- Reset - A result of resetting a host.
- Downgrade - A result of policy downgrade on hosts.

## UACC

Defines the default access authority for the resource. The access authority indicates the access that is granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted. If an access request violates an access rule, a record is written to the audit log.

## GHNODE Class

Each record in the GHNODE class defines a host group-a group of hosts (HNODE objects). You must create a HNODE class record for each host before adding it to a GHOST record.

This class is used to manage policy deployment and assignment.

The key of the GHNODE class record is a logical name for the host group.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Access**  
Defines the access authority that the accessor has to the resource.

Use the access parameter with the authorize or authorize- command to modify the ACL.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **CRITERIA**

Defines the criteria that the DMS uses to automatically add hosts to this host group. You can specify criteria that matches or excludes the following HNODE properties: ATTRIBUTES, COMMENT, HNODE\_INFO, HNODE\_IP, HNODE\_VERSION, NODE\_TYPE

For example, the HNODE records for Windows endpoints have the property HNODE\_INFO=Windows. If the CRITERIA property for a GHNODE record has the value of HNODE\_INFO=Windows, the DMS automatically adds any new Windows HNODE to the GHNODE.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **MEMBERS**

The list of objects from the HNODE class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **OWNER**

Defines the user or group that owns the record.

#### **POLICIES**

The list of policies that should be deployed on this object.

#### **POLICYASSIGN**

Defines the list of policies that are assigned to this object.

Display name: Assigned Policies

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**



Granted access requests.

- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## GHOST Class

Each record in the GHOST class defines a group of hosts. You create a HOST class record for each host before adding it to a GHOST record. The services must be defined to the system using the /etc/services file (for UNIX), \system32\drivers\etc\services file (for Windows), or another service name resolution method. When authorizing services, you can identify the services by their port numbers in the TCP/IP protocol rather than by their names. When adding services, you can identify the services by their port numbers in the TCP/IP protocol rather than by their names. You then explicitly connect records of the HOST class to the GHOST record to group them.

GHOST records define access rules that govern the access other stations (hosts) belonging to the group of hosts have to the local host when using Internet communication. For each client group (GHOST record), the INETACL property lists the service rules that govern the services the local host may provide to hosts belonging to the client group.

The key of the GHOST class record is the name of the GHOST record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **INETACL**

Defines the services the local host is allowed to provide to the group of client hosts and what their access types are.

Each element in the access control list contains the following information:

- **Services reference**

A reference to a service (a port number or name). To specify all the services, enter an asterisk (\*) as the services reference.

Privileged Access Manager supports dynamic port names as specified in the /etc/rpc file (for UNIX) or \etc\rpc file (for Windows).

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access(*type-of-access*), service, and stationName parameters with the authorize[-] command to modify accessors and their access types in the INETACL property.

- **INSERVNGE**

Specifies the range of services that the local host provides to the group of client hosts.

Performs a similar function to the INETACL property.

Use the service(*serviceRange*) parameter with the authorize[-] command to modify accessors and their access types in the INSERVNGE property.

- **MEMBERS**

The list of objects from the HOST class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

- **OWNER**

Defines the user or group that owns the record.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## GPOLICY Class

Each record in the GPOLICY class defines a logical policy. It contains information about the policy versions (POLICY objects) that belong to this policy and the hosts and host groups it is assigned to.

The key of the GDEPLOYMENT class is the name of the logical policy.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.  
Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GHNODEASSIGN**  
Defines the host groups this policy is assigned to.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **HNODEASSIGN**  
Defines the hosts this policy is assigned to.
- **LATEST\_FINALIZED\_VERSION**  
Defines the name of the latest policy version (POLICY object) that is finalized.
- **LATEST\_VERSION**  
Defines the name of the latest policy version (POLICY object) associated with this policy.
- **MEMBERS**  
The list of objects from the POLICY class (policy versions) that are members of the group.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres`, and `newres` commands to modify this property.
- **NACL**

The NACL property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

### Accessor

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

## NOTIFY

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## OWNER

Defines the user or group that owns the record.

## PACL

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

### NOTE

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

## POLICY TYPE

A value representing the group policy type. Valid values are:

- **None**
- **Login** Specifies that the policy is a UNAB login policy.
- **Configuration** Specifies that the policy is a UNAB configuration policy.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

**SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

**SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

**UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

**UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

**UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

**WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**GROUP Class**

Each record in the GROUP class defines a group of users in the database.

The key of each GROUP class record is the name of the group.

**NOTE**

The properties of profile groups apply to each user associated with the profile group. However, if the same property is specified in a user (USER or XUSER) record, the user record overrides those in the profile group record.

You can change most of these properties from the Privileged Access Manager Endpoint Management, or by using the selang command chgrp.

**NOTE**

Usually, and unless otherwise indicated, to change a property using ch[x]grp, you use the property name as the command parameter.

You can view all properties from the Privileged Access Manager Endpoint Management, or by using the selang command showgrp.

- **APPLS**

(Informational) Displays the list of applications that the accessor is authorized to access. Used by CA SSO.

- **AUDIT\_MODE**

Defines the activities that Privileged Access Manager records in the audit log. You can specify any combination of the following activities:

- No logging
- All activities recorded in the trace file
- Unsuccessful login attempts
- Successful logins
- Failed access attempts to resources protected by Privileged Access Manager
- Successful accesses to resources protected by Privileged Access Manager
- Interactive logins

#### **NOTE**

This property corresponds to the audit parameter of the `ch[x]usr` and `ch[x]grp` commands. You can use `AUDIT_MODE` for a `GROUP` or `XGROUP` to set the audit mode for all members of the group. However, you cannot use `AUDIT_MODE` to set the audit mode for group members if the audit mode of a user is defined in a `USER` record, `XUSER` record, or profile group.

- **AUTHNMTHD**  
(Informational) Displays the authentication method or methods to be used with the group record; from method 1 to method 32, or none. Used by CA SSO.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **EXPIRE\_DATE**  
Defines the date on which an accessor becomes invalid. A value for the `EXPIRE_DATE` property in a user record overrides a value in a group record.  
**Note:** This property corresponds to the `expire[-]` parameter of the `ch[x]usr` and `ch[x]grp` commands.
- **FULLNAME**  
Defines the full name associated with an accessor. Privileged Access Manager uses the full name to identify the accessor in audit log messages, but not for authorization.  
`FULLNAME` is an alphanumeric string. For groups, the maximum length is 255 characters. For users, the maximum length is 47 characters.
- **GAPPLS**  
Defines the list of application groups that the group is authorized to access. Used by CA SSO.
- **GROUP\_MEMBER**  
Defines the groups that are members of this group.
- **GROUP\_TYPE**  
Specifies the group authority attributes. Each of these attributes corresponds to the parameter of the same name in the `ch[x]grp` command. A group can have one or more of the following authority attributes:
  - **ADMIN**  
Specifies whether a user who belongs to the group can perform administrative functions, similar to root in the UNIX environment.
  - **AUDITOR**  
Specifies whether a user who belongs to the group can monitor the system, list information in the database, and can set the audit mode for existing records.
  - **OPERATOR**

Specifies whether a user who belongs to the group can list everything in the database and can use the `secons` utility.

- **PWMANAGER**

Specifies whether a user who belongs to the group can modify the password settings of other users and can enable a user account that the `serevu` utility has disabled.

- **SERVER**

Specifies whether a process can ask users who belong to the group for authorization and can issue the `SEOSROUTE_VerifyCreate` API call.

- **HOMEDIR**

Defines the path of the home directory assigned to a new group member.

Use the `homedir` parameter with the `chgrp`, `editgrp`, or `newgrp` command to modify this property.

**Limit:** 255 alphanumeric characters

- **INACTIVE**

Defines the number of days of inactivity that must pass before the system changes the status of a user to inactive. If the account status is inactive, the user cannot log in.

A value for the **INACTIVE** property in a **USER** record overrides a value in a **GROUP** record. Both override the **INACT** property in the **SEOS** class record.

**NOTE**

Privileged Access Manager does not store the status; it calculates the status dynamically. To identify inactive users, compare the **INACTIVE** value with the **LAST\_ACC\_TIME** value of the user.

**INACTIVE** is part of the profile feature.

- **MAXLOGINS**

Defines the maximum number of concurrent logins that a user is allowed. A zero value indicates that the user can have any number of concurrent logins.

A value for the **MAXLOGINS** property in a user record overrides a value in a group record. Both override the value of **MAXLOGINS** in the **SEOS** class record.

**MAXLOGINS** is part of the profile feature.

- **MEMBER\_OF**

Defines the groups that this group is a member of.

- **OWNER**

Defines the user or group that owns the record.

- **PASSWDRULES**

Specifies the password rules. This property contains several fields that determine how Privileged Access Manager handles password protection. For a complete list of the rules, see the modifiable property **PROFILE** of the **USER** class. Use the `passwordparameter` and the `rules` or `rules-` option with the `setoptions` command to modify this property.

**PASSWDRULES** is part of the profile feature.

- **POLICYMODEL**

Specifies the **PMDB** that receives new passwords when you change user passwords with the `sepass` utility. The passwords are *not* sent to the Policy Model defined by the `parent_pmd` or `passwd_pmd` configuration settings if a value is entered for this property.

**Note:** This property corresponds to the `pmdb[-]` parameter of the `ch[x]usr` and `ch[x]grp` commands.

**POLICYMODEL** is part of the profile feature.

- **PROFUSR**

Displays a list of the users associated with this profile group.

- **PWD\_AUTOGEN**

Indicates whether the group password is automatically generated. The default is `no`. Used by CA SSO.

- **PWD\_SYNC**

Indicates whether the group password is automatically kept identical for all group applications. The default is `no`. Used by CA SSO.

- **PWPOLICY**

Defines the record name of the password policy for the group. A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. The default is no validity check. Used by CA SSO.

- **RESUME\_DATE**

Defines the date on which a suspended USER account becomes unsuspended.

RESUME\_DATE and SUSPEND\_DATE work together.

**NOTE**

This property corresponds to the resume[-] parameter of the ch[x]usr and ch[x]grp commands. RESUME\_DATE is part of the profile feature.

- **REVACL**

Displays the access control lists of the accessor.

- **SHELL**

(UNIX only) The shell program that is assigned to a new UNIX user when the user is a member of this group.

Use the shellprog parameter with the chxgrp command to modify this property.

- **SUBGROUP**

Displays the list of groups that have this group as a parent.

- **SUPGROUP**

Defines the name of the parent group (superior group).

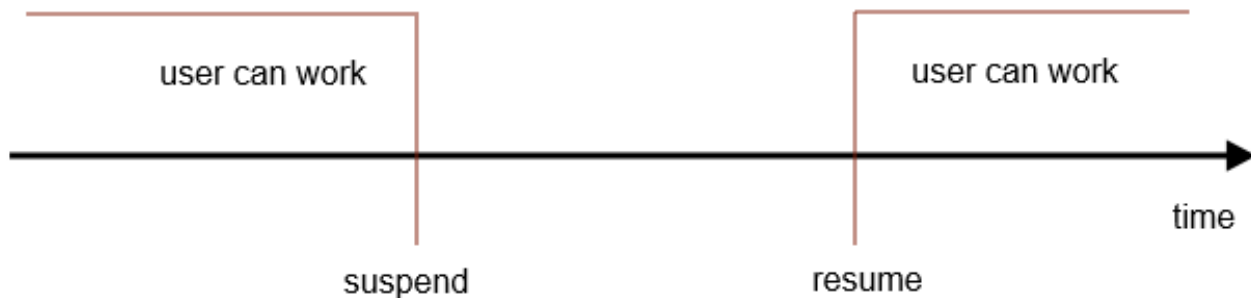
Use the parent[-] parameter with the ch[x]grp command to modify this property.

- **SUSPEND\_DATE**

Defines the date on which a user account is suspended and so becomes invalid.

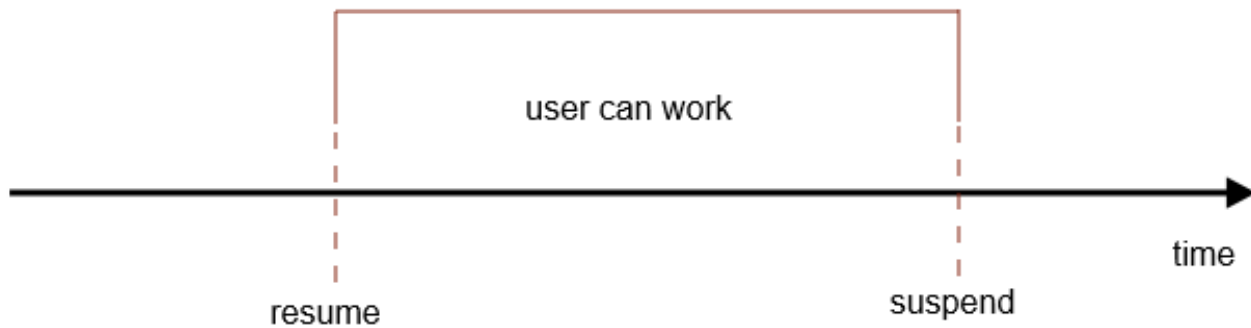
If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.

**Figure 53: suspend\_date3a**



If a user has a resume date that is earlier than the suspend date, the record is also invalid *before* the resume date. The user can work only between the resume and suspend dates.



**Figure 54: suspend\_date4a**

A value for the SUSPEND\_DATE property in a user record overrides the value in a group record.

**NOTE**

This property corresponds to the suspend[-] parameter of the ch[x]usr and ch[x]grp commands.

- **SUSPEND\_WHO**  
Displays the administrator who activated the suspend date.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **USERLIST**  
Defines the users that belong to the group.  
The user list that is contained in this property can be different from the one in the native environment USERS property.  
Use the join[x][-] commands to modify this property.

## GSUDO Class

Each record in the GSUDO class defines a group of actions that Task Delegation-the DO (sesudo)-allows a user to execute or prevents a user from executing. You must create a SUDO class record for each action before adding it to a GSUDO record.

Use GSUDO to define access rules for a group of SUDO resources rather than specifying the same access rule for each resource. You must explicitly connect records of the SUDO class to the GSUDO record in order to group them.

The key of the GSUDO class record is the name of the group.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.
- **MEMBERS**  
The list of objects from the SUDO class that are members of the group.  
Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **OWNER**

Defines the user or group that owns the record.

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

#### **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

#### **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## GTERMINAL Class

Each record in the GTERMINAL class defines a group of terminals. You must create a TERMINAL class record for each terminal before adding it to a GTERMINAL record. You must then explicitly connect records of the TERMINAL class to the GTERMINAL record in order to group them.

Terminal groups are useful when defining access rules. You can use a single command to specify an access rule for a group of terminals rather than having to specify the same access rule for each terminal. Similarly, you may apply a rule for a group of terminals by a single command to a group of users.

The key of the GTERMINAL class record is the name of the terminal group.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **MEMBERS**

The list of objects from the TERMINAL class that are members of the group.

Use the `mem+` or `mem-` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

### Accessor

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

### OWNER

Defines the user or group that owns the record.

### RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## GWINSERVICE Class

Each record in the GWINSERVICE class defines a group of Windows Services. Use records in the GWINSERVICE class to define access rules for a group of Windows Services.

The key of a GWINSERVICE class record is the name of the GWINSERVICE record.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

### **Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

### **OWNER**

Defines the user or group that owns the record.

### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

**UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

**UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

**HNODE Class**

The HNODE class contains information about the organization's Privileged Access Manager hosts. Each record in the class represents a node in the enterprise.

This class is used to manage the information uploaded from the various PMDBs and endpoints and stored on the DMS.

The key of the HNODE class record is the actual host name for an endpoint (for example, myHost.ca.com) or the PMDB name for a Policy Model node (for example, myPMD@myHost.ca.com).

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **ATTRIBUTES**

Defines the custom criteria that the DMS uses to assess if the host is automatically added to a host group.

**NOTE**

The DMS also examines the following HNODE properties to assess if a host should be automatically added to a host group: `COMMENT`, `HNODE_INFO`, `HNODE_IP`, `HNODE_VERSION`, `NODE_TYPE`

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **COMPLIANT\_UPDATE\_TIME**

(Informational) Displays the date and time when the status was last changed.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **EFFECTIVE\_POLICIES**

Defines the list of policy versions that should be deployed on this object.

Display name: Effective Policies

- **GHNODES**

Defines the list of host groups this object is a member of.

Display name: node groups

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **HNODE\_IP**

The IP address of the host.

Display name: IP

- **HNODE\_KEEP\_ALIVE**

Defines the last time the HNODE sent a heartbeat to the Distribution Host.

Display name: Last Heartbeat

- **HNODE\_EVENTS**

Displays a list of strings representing health recovery events that occurred on the endpoint. Health recovery events are, for example, restarting of an agent due to critical memory threshold breach, or bypassing of a program that deteriorates the performance of the endpoint.

- **HNODE\_INSTALL\_STATUS**

Displays the installation status of an endpoint. You can search endpoints by status in Privileged Access Manager Enterprise Management under World View.

**Values:** Success, Failure, Pending Reboot, Upgrading.

Display name: Install Status.

- **HNODE\_BYPASS\_EXIST**

Displays whether the endpoint is in bypass mode as a measure of precaution. In bypass mode, Privileged Access Manager policy handling is temporarily reduced. If this value is No then the endpoint is fully operational.

**Value:** Yes or No

Display name: Bypass exist.

- **LOGIN**

Defines the default access type to the host.

Display name: LOGIN

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

**NODE\_INFO**

(Informational) Specifies details of the node OS.

**NODE\_TYPE**

(Informational) Defines the type of Privileged Access Manager installation on the host. Valid values are:

- ACUCA ControlMinder for UNIX
- ACWCA ControlMinder for Windows
- UNABUNIX Authentication Broker (UNAB)

**NOTE**

A HNODE record can have a value of both ACU and UNAB for the NODE\_TYPE property.

**NODE\_VERSION****NOTE**

(Informational) Defines the Privileged Access Manager version installed on the host. The version number is preceded by the NODE\_TYPE. Example: ACU:12.50-00.647

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

**PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the *selang authorize* command to add programs, accessors, and their access types to a PACL. You can use the *authorize-* command to remove accessors from a PACL.

**PARENTS**

(Informational). The list of PMDBs that are the parents of the node in the propagation tree (also defined by the *parent\_pmd* configuration setting).

**POLICYASSIGN**

Defines the list of policies that are assigned to this object.

Display name: Assigned Policies

**POLICY**

The status of each of the policies listed in the POLICIES property. The value of the property is a structure with the following fields:

- **nNAME**  
Object ID of the POLICY object. Same as the value of the POLICIES property.
- **STATUS**  
An integer representing one of the following:
  - DeployedPolicy was deployed successfully on endpoint.
  - Deployed with FailuresPolicy was deployed with one or more rules from the deployment script failing to execute on the endpoint.
  - UndeployedPolicy was undeployed successfully from endpoint.



**Note:** If a policy is undeployed, no status appears for the host (that is, the status is empty).

- Undeployed with FailuresPolicy was undeployed with one or more rules from the undeployment script failing to execute on the endpoint.

- Failed DeploymentPolicy failed to deploy due to an error in the deployment script.

**Note:** This status can appear only if policy verification is enabled. Otherwise, policyfetcher deploys a policy even if the policy contains errors (Deployed with Failures status).

- UnknownPolicy status is unknown.
- Deploy PendingWaiting for a prerequisite policy to be deployed or the policy contains an undefined or unresolved variable.
- Undeploy PendingWaiting for a dependent policy to be undeployed.
- Out of SyncThe policy contains a variable and the variable value has changed on the endpoint.
- Not ExecutedPolicy verification found one or more errors with the policy.
- QueuedObsolete (for backward compatibility only.)
- TransferredObsolete (for backward compatibility only.)
- Transferred FailedObsolete (for backward compatibility only.)
- Signature FailedObsolete (for backward compatibility only.)

- **deviation**

A value representing whether there is a policy deviation on this node. Valid values are:

- Yes
- No
- Unset

- **dev\_time**

Last deviation status update time.

- **ptime**

Last policy status update time.

- **updater**

The name of the user that deployed or removed the policy.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## SUBSCRIBER\_STATUS

The status of the node per parent. The value of the property is a structure with the following fields:

- **oidSubs**  
Object ID of the HNODE object. Same as the value of the SUBSCRIBERS property.
- **status**  
A value representing one of the following statuses:
  - Available
  - Unavailable
  - Sync (synchronizing)
  - Unknown
- **stime**  
Last status update time.

## SUBSCRIBERS

The list of subscribers of the node in the propagation tree. Updating this property, implicitly updates the PARENTS property with the value of the HNODE object name.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UNAB\_ID

(Informational) Displays the UNAB host ID for reporting purposes.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## HOLIDAY Class

Each record in the HOLIDAY class defines one or more periods when users need extra permission to log in.

Each user has the same access for all the time periods in a record. This means that if you include more than one holiday period in a holiday record, you cannot allow a user to log in during some of those periods and prevent that user from logging in during others. For example, if you want to allow a specific user to log in during New Year's Day but not during Christmas, then the two holidays must be defined in different records.

If you do not specify the year, the holiday is considered annual.

You can override HOLIDAY class restrictions for individual users by specifying the IGN\_HOL attribute in the newusr, chusr, or editusr command.

The key of the HOLIDAY class record is the name of the HOLIDAY record.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **HOL\_DATE**

Specifies the period during which users cannot log in.

The following rules apply to the HOL\_DATE property:

- If you do not specify a year, it means the period or holiday is annual. You can specify the year with two digits or four digits, for example: 99 or 1999.
- If you do not specify a start time then the start of the day (midnight) is used; and if you do not specify an end time then the end of the day (midnight) is used.
- If you do not specify an interval of time, but only a date, then the holiday lasts for one whole day.

Use the dates parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **NACL**

The NACL property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

## **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## **SECLABEL**

Defines the security label of a user or resource.

### **NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

## **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## **HOST Class**

Each record in the HOST class defines the access that a host has to the local computer connected by IPv4 or IPv6.

Privileged Access Manager resolves the addresses of host names that you add to the HOST class. This means that the names must appear in the operating system hosts file, or must be defined to NIS or DNS.

For each HOST record, the INETACL property defines the services the local host can provide to that host.

Privileged Access Manager permits aliases for a host name, but records that represent aliases are not used for authorization checks. You must know the canonical name of a host for Privileged Access Manager to protect the connection with that host.

Privileged Access Manager resolves a hostname by one IP address. If multiple IP addresses are configured for one hostname, then use one of the following classes:

- GHOST
- HOSTNET
- HOSTNP

The key of the HOST class record is the name of the host.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Nonmodifiable properties are marked *informational*.

- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
The list of GHOST or CONTAINER records a resource record belongs to.  
To modify this property in a HOST class record, change the MEMBERS property in the appropriate CONTAINER or GHOST record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **INETACL**  
Defines the services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:
  - **Services reference**  
A reference to a service (a port number or name). To specify all the services, enter an asterisk (\*) as the services reference.  
Privileged Access Manager supports dynamic port names as specified in the `/etc/rpc` file (for UNIX) or `\etc\rpc` file (for Windows).
  - **Access**  
Defines the access authority that the accessor has to the resource.  
Use the `access(type-of-access)`, `service`, and `stationName` parameters with the `authorize[-]` command to modify accessors and their access types in the INETACL property.
- **INSERVNGE**  
Specifies the range of services that the local host provides to the group of client hosts.  
Performs a similar function to the INETACL property.  
Use the `service(serviceRange)` parameter with the `authorize[-]` command to modify accessors and their access types in the INSERVNGE property.
- **OWNER**  
Defines the user or group that owns the record.
- **RAUDIT**  
Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:
  - **all**

All access requests.

- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the `chres` and `chfile` commands to modify the audit mode.

- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **WARNING**  
Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example:** Prevent incoming connections to Privileged Access Manager endpoint from a restricted remote host using Telnet.

**Step 1:** Add a remote host ([My\\_Remote\\_Host.example.com](#)) in `/etc/hosts`. Run the following command at the command prompt.

```
vi /etc/hosts
```

**Step 2:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildda -h
```

**Step 3:** Run the following command at the command prompt to verify that the remote host ([My\\_Remote\\_Host.example.com](#)) is added to `/etc/hosts`.

```
./sebuildda -H
```

**Step 4:** Define a remote host ([My\\_Remote\\_Host.example.com](#)) from which we prevent incoming Telnet connections.

```
PAMSC> nr HOST My\_Remote\_Host.example.com
```

**Step 5:** Set a rule that prevents incoming connections from the remote host ([My\\_Remote\\_Host.example.com](#)) using Telnet.

```
PAMSC> authorize HOST My\_Remote\_Host.example.com service(telnet) access(none)
```

**Step 6:** Try connecting from the remote host to the Privileged Access Manager endpoint using Telnet. The connection fails but other connections are not affected.

To deny any type of connection from a remote host (([My\\_Remote\\_Host.example.com](#))), set the following rule.

```
PAMSC> authorize HOST My\_Remote\_Host.example.com service(*) access(none)
```

## HOSTNET Class

Each record in the HOSTNET class defines a group of hosts on a particular network. HOSTNET records define rules that govern the access other hosts in the group have to the local host when using IPv4 communication.

### NOTE

Privileged Access Manager access rules for IP communication apply only to IPv4. They do not control access by IPv6.

The INMASKMATCH determines which other hosts are subject to a HOSTNET record. The INETACL property defines which services the local host can provide to those hosts.

The key of the HOSTNET class record is the name of the HOSTNET record.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **INETACL**

Defines the services that the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:

- **Services reference**

A reference to a service (a port number or name). To specify all the services, enter an asterisk (\*) as the services reference.

Privileged Access Manager supports dynamic port names as specified in the `/etc/rpc` file (for UNIX) or `\etc\rpc` file (for Windows).

- **Access**

Defines the access authority that the accessor has to the resource.

Use the `access(type-of-access)`, `service`, and `stationName` parameters with the `authorize[-]` command to modify accessors and their access types in the INETACL property.

- **INSERVNGE**

Specifies the range of services that the local host provides to the group of client hosts.

Performs a similar function to the INETACL property.

Use the `service(serviceRange)` parameter with the `authorize[-]` command to modify accessors and their access types in the `INSERVRange` property.

- **INMASKMATCH**

Defines the group of hosts to which this HOSTNET record applies. The property contains mask and match values, which are applied to the IP address of the requesting host to determine whether the requesting host belongs to the group.

The INMASKMATCH property only supports addresses that are in IPv4 format .

**NOTE**

This property corresponds to the mask and match parameters of the `chres` command.

- **OWNER**

Defines the user or group that owns the record.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example:** Prevent incoming connections to Privileged Access Manager endpoint from remote hosts in a given subnet.

**Step 1:** Add remote hosts in `/etc/hosts`. Run the following command at the command prompt.

```
vi /etc/hosts
```

**Step 2:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildla -h
```

**Step 3:** Run the following command at the command prompt to verify that the remote hosts are added to `/etc/hosts`.

```
./sebuildla -H
```



**Step 4:** Create the given rule. Assume 'engineering' defines the group of hosts in the subnet (10.131.33) belonging to engineering department. As per the rule, all incoming connections from IP addresses (10.131.33.\*) are considered using the 'Mask' value.

```
PAMSC> nr HOSTNET engineering mask(255.255.255.0) match(10.131.33.0)
```

**Step 5:** Set a rule that prevents incoming connections from remote hosts in a given subnet using Telnet.

```
PAMSC> authorize HOSTNET engineering service(telnet) access(none)
```

**Step 6:** Try connecting from the remote host (within the subnet) to the Privileged Access Manager endpoint using Telnet. The connection fails but other connections are not affected.

To deny any type of connection from a remote host within a given subnet, set the following rule.

```
PAMSC> authorize HOSTNET engineering service(*) access(none)
```

## HOSTNP Class

Each record in the HOSTNP class defines a group of hosts that have similar host names. HOSTNP records define access rules that govern the access other stations (hosts) that match name pattern in the record have to the local host when using IPv4 or IPv6. For each mask (HOSTNP record), the INETACL property lists the service rules that govern the services that the local host might provide to the group of hosts.

The key of the HOSTNP class record is the name pattern that is used to filter the host names of the hosts that are protected by this HOSTNP record.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.
- **INETACL**  
Defines the services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:
  - **Services reference**

A reference to a service (a port number or name). To specify all the services, enter an asterisk (\*) as the services reference.

Privileged Access Manager supports dynamic port names as specified in the `/etc/rpc` file (for UNIX) or `\etc\rpc` file (for Windows).

- **Access**

Defines the access authority that the accessor has to the resource.

Use the `access(type-of-access)`, `service`, and `stationName` parameters with the `authorize[-]` command to modify accessors and their access types in the `INETACL` property.

- **INSERVNGE**

Specifies the range of services that the local host provides to the group of client hosts.

Performs a similar function to the `INETACL` property.

Use the `service(serviceRange)` parameter with the `authorize[-]` command to modify accessors and their access types in the `INSERVNGE` property.

- **OWNER**

Defines the user or group that owns the record.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. `RAUDIT` derives its name from Resource `AUDIT`. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example:** Prevent incoming connections to Privileged Access Manager endpoint from a restricted remote host, using host name pattern.

**Step 1:** Add remote hosts in `/etc/hosts`. Run the following command at the command prompt.

```
vi /etc/hosts
```

**Step 2:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildla -h
```

**Step 3:** Run the following command at the command prompt to verify that the remote hosts are added to `/etc/hosts`.

```
./sebuildla -H
```

**Step 4:** Define remote hosts (using host name pattern) from which we prevent incoming Telnet connections.

```
PAMSC> nr HOSTNP My_Remote_*
```

**Step 5:** Set a rule that prevents incoming connections from remote hosts using Telnet.

```
PAMSC> authorize HOSTNP My_Remote_* service(telnet) access(none)
```

**Step 6:** Try connecting from a remote host (with the defined host name pattern) to the Privileged Access Manager endpoint using Telnet. The connection fails but other connections are not affected.

To deny any type of connection from remote hosts, set the following rule.

```
PAMSC> authorize HOSTNP My_Remote_* service(*) access(none)
```

## KMODULE Class

Each record in the KMODULE class defines a kernel module of the operating system.

If a module is defined in the KMODULE class, any call to the operating system to load or unload that module, causes Privileged Access Manager to check the authorizations defined for that module.

The key of a KMODULE record is the name of the kernel module being protected.

Each KMODULE record contains the following properties:

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information: Accessor Defines an accessor. Access Defines the access authority that the accessor has to the resource. Use the access parameter with the authorize or authorize-command to modify the ACL. Valid access authorities for KMODULE records are load and unload.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **FILEPATH**

Defines a list of absolute paths to files, each of which contains a kernel module. Separate each file path with a colon (:).

Use more than one file path if you have different versions of the same module.

If no file path is provided, Privileged Access Manager does not perform file path checking on kernel module load.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **NACL**

The NACL property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **OWNER**

Defines the user or group that owns the record.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the via(*pgm*) parameter with the selang authorize command to add programs, accessors, and their access types to a PACL. You can use the authorize- command to remove accessors from a PACL.

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## SIGNATURE

Displays the unique values for kernel module files defined in the filepath property .

Privileged Access Manager calculates the signatures of kernel modules when it starts up, and when a KMODULE record is changed using selang commands. You can set the signatures yourself using the command seretrust -m.

### NOTE

Privileged Access Manager uses the SIGNATURE property for Linux systems only.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## LOGINAPPL Class

### Valid on UNIX

Each record in the LOGINAPPL class defines a login application, identifies who can use the program to log in, and controls the way the login program is used.

The key of the LOGINAPPL class record is the name of the application, that is, a logical name that represents a login application. This logical name is associated, in the LOGINPATH property, with the full path name of the executable.

Privileged Access Manager can also control and protect generic login applications; this means that you can protect groups of login applications that match a certain rule with a generic pattern. To define a generic login application with `selang`, use the same commands as setting regular login restrictions, except the `LOGINPATH` parameter, which should include a generic path composed of a regular expression using one or more of the following characters: `[, ], *, ?`.

Privileged Access Manager presets the property values for records in the `LOGINAPPL` class for standard login programs. You should list and verify the existing settings before making any changes.

### **WARNING**

`LOGINAPPL` does not use the `_default` entry.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **LOGINFLAGS**

Controls special features of the login application, including changes in device number and decrements to the grace logins number. Valid values are:

- **execlogin**-Specifies that the login trigger is the first EXEC action that a process performs.

- **loginprefix**-Specifies that Privileged Access Manager adds the `LOGINAPPL` resource name as the prefix to the logged-in user name. For example, if you set this property and a user named `user1` schedules a CRON task, when CA Privileged Access Manager detects the CRON task login it sets the user name to `USR_SBIN_CRON_user1`.

**Note:** Privileged Access Manager does not add the `LOGINAPPL` resource name as a prefix to `root`.

- **nograce**-Indicates that grace logins should not be decremented when users log in through this application.

- **nograceroot**-Indicates that grace logins should not be decremented when root logs in through this application.

- **nologin**-Ensures that a login is entered for the user only. The login is not logged for parent programs.

A program like `rlogin` on some platforms causes `rlogin` to trigger the login and close the login sequence itself; this results in an actual login logged for root. After performing the login, `rlogin` forks to another program to perform the actual login.

This problem is apparent if you use a login program such as `rlogin` or `telnet` and run `seaudit -a`. You see that there are also login records for the same login with root as the uid.

- **pamlogin**-Indicates that Privileged Access Manager PAM login interception is used when users log in through this application.

Use the `loginflags` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **LOGINMETHOD**

Indicates whether the login application is a pseudo login program for the purposes of Privileged Access Manager protection. Valid values are:

- **normal**-Indicates that this login application executes `setuid` and `setgid` calls itself. `seosd` checks the rules of the specified program.
- **pseudo**-Indicates that this login application calls another program to execute `setuid` and `setgid` calls. `seosd` checks the rules on the other program.

Use the `loginmethod` parameter with the `chres`, `editres`, or `newres` command to modify this property.

#### **WARNING**

We recommend that you not modify this preset property.

- **LOGINPATH**

The full path (or generic path) to the login application.

Use the `loginpath` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **LOGINSEQUENCE**

Defines the sequence of `seteuid`, `setuid`, `setgid`, and `setgroups` events that `seosd` processes to set the user from the daemon starting the login process (usually `inetd` under `root`) to the user who is actually logged on. You can define up to eight system events.

The login interception sequence always starts with `setgid` or `setgroups` events, which are called *triggers*. It ends with a `setuid` event that changes the user's identity to the real user who logged in.

To successfully accomplish login, the program needs to perform all the specified processes in sequence starting with `setgroups` or `setgid` and ending with `setuid` or `seteuid`.

Setting the right `LoginSequence` for a program is a difficult task. Most login programs work well with the default `SGRP,SUID` setting; this setting means the program issues a `setgroups` system call and then a `setuid` command to change the user's identity to the target user.

However, if the `SGRP, SUID` setting does not work, you must use the following flags to specify the proper order:

- **SEID**-First `seteuid` event
- **SUID**-First `setuid` event
- **SGID**-First `setgid` event
- **SGRP**-First `setgroup` event
- **FEID**-Second `seteuid` event
- **FUID**-Second `setuid` event
- **FGID**-Second `setgid` event
- **FGRP**-Second `setgroup` event
- **N3EID**-Third `seteuid` event
- **N3UID**-Third `setuid` event
- **N3GID**-Third `setgid` event
- **N3GRP**-Third `setgroup` event

#### **WARNING**

You must use the flags to specify the correct login sequence. However, you can specify the flags in any order within the `LOGINSEQUENCE` parameter. For example, `SGRP, SEID, FEID, N3EID` is identical to `N3EID, FEID, SGRP, SEID`.

#### **NOTE**

If you do not know the sequence of system calls that the login program performs, you can view the trace and look for the `setuid` event that changed the user to the target uid, and then look at prior trace events starting with the first `setgid` or `setgroups` event.

For example, if you there is one `setgroups` event and then only the third `setuid` call sets the target user, you must set `LOGINSEQUENCE` to `SGRP,SUID,FUID,N3UID`. You can specify these flags in any order:

```
SETGRPS : P=565302 to 0,2,3,7,8,10,11,250,220,221,230
SUID > P=565302 U=0 (R=0 E=0 S=0 ) to (R=0 E=0 S=0 ) ( ) BYPASS
SUID > P=565302 U=0 (R=0 E=0 S=0 ) to (R=0 E=0 S=-1 ) ( ) BYPASS
```

LOGIN : P=565302 User=target Terminal=mercuryThe SETGRPS process indicates the trigger.The first SUID command should be discounted because you can see that the root simply changed back to root, not the trigger user. (This is the SUID in the sequence.)The second SUID command should be discounted as well because you can see that the root changed back to root, not the trigger user. (This is the FUID in the sequence.)The LOGIN event is the actual SETUID event causing the login. (Because it is the third event, it is the N3UID flag in the sequence.)

Use the loginsequence parameter with the chres, editres, or newres command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also *ACL*, *CALACL*, *PACL*. Each entry in the *NACL* contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

**RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. *RAUDIT* derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

**UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the *ACL* of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

**UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.



**UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

**WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**MFTERMINAL Class**

Each record in the MFTERMINAL class defines a Mainframe computer that is used to administer Privileged Access Manager. It has the same characteristics as the TERMINAL class, but is not intercepted by Privileged Access Manager.

The key of the MFTERMINAL class is the name of the mainframe computer.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.  
Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.
- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

**Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

## NOTIFY

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

## OWNER

Defines the user or group that owns the record.

## PACL

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### NOTE

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the `label[-]` parameter of the `chres` and `ch[x]usr` commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

### WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## POLICY Class

Each record in the POLICY class defines the information required to deploy and undeploy a policy version. It includes a link to the RULESET objects that contain a list of the `selang` commands for deploying and undeploying the policy. When the policy is deployed, the `deploy selang` command is run, which executes all of the commands that define the policy and are stored in the linked RULESET object. When the policy is undeployed, the `deploy- selang` command is run, which executes all of the commands that refine policy undeployment and are stored in the linked RULESET object.

The key of the POLICY class is the name of the policy followed by the hash symbol (#) and a two-digit version number. For example, `mypolicy#13`.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **EFFECTS\_ON**  
Defines the list of hosts (HNODE objects) on which this policy is effective (should be deployed).
- **FINALIZE**

Specifies whether this policy version is finalized (can be deployed).

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to or the GPOLICY object this policy version belongs to.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **HNODES**

(Informational). The list of Privileged Access Manager nodes which should have this policy deployed.

- **NACL**

The NACL property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **OWNER**

Defines the user or group that owns the record.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the via(*pgm*) parameter with the selang authorize command to add programs, accessors, and their access types to a PACL. You can use the authorize- command to remove accessors from a PACL.

#### **POLICY\_BASE\_NAME**

Defines the name of the GPOLICY object this policy version is a member of.

#### **POLICY\_VERSION**

Defines the version number of this policy version.

#### **POLICY\_TYPE**

Defines the policy type. Valid values are:

- None
- Login Specifies that the policy is a UNAB login policy.
- Configuration Specifies that the policy is a UNAB configuration policy.

## **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## **RULESETS**

The list of RULESET objects which define the policy.

## **SECLABEL**

Defines the security label of a user or resource.

### **NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## **SIGNATURE**

A hash value based on signatures of the RULESET objects associated with the policy.

## **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

## **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## **VARIABLES**

(Informational) Displays all versions of the variables in the policy.

## **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## PROCESS Class

Each record in the PROCESS class defines a program—an executable file—that runs in its own address space and that needs to be protected from being killed or getting debugged. Major utilities and database servers are good candidates for such protection since these processes are the main targets for denial-of-service attacks.

**Note:** When defining a program in the PROCESS class, we recommend that you also define it in the FILE class. This protects the executable by preventing someone from modifying (replacing or corrupting) the executable without authorization.

The PROCESS class now contains the following two access control attributes:

- **read**  
Allows the process to be killed
- **attach**  
Allows the process to be attached

Both the attributes are mutually independent and can be set together.

**Note:** The ATTACH attribute of the PROCESS class that is introduced in the current release is not available in the Endpoint Management UI. The ATTACH access right is not applied to the rule even if the access right All is selected for the PROCESS class objects, in the Endpoint Management UI.

### KILL Attribute

Privileged Access Manager can protect against three terminate (kill) signals: the regular terminate signal (SIGTERM) and the two signals that an application cannot mask (SIGKILL and SIGSTOP):

Environment	Signal	Number
Windows	KILL	Win32 API
UNIX	Terminate Process	9
UNIX and Windows	STOP	Machine Dependent
UNIX and Windows	TERM	15

Other signals, such as SIGHUP or SIGUSR1, are passed to the process that they target and that process decides whether to ignore the terminate signal or whether to react to it in some way.

The key of the PROCESS class record is the name of the program the record protects. Specify the full path.

### ATTACH Attribute

The ATTACH attribute of the PROCESS class authorizes the defined process for being attached by other processes for debugging or tracing; provided those processes are running under an authorized user.

**Note:** Only the Linux and AIX operating systems support the ATTACH attribute.

To define the ATTACH attribute using the PROCESS class, create a record for a process that you want to authorize. Create the record without an owner and any access right defined. Using a Selang rule, you can authorize the process that you have created to be attached by any other process running under root.

### WARNING

If you had denied KILL access to a process and allowed ATTACH access to the same process, then the process can be killed by a process which has the access right ATTACH.

### PROCESS Class Properties

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Properties marked as *informational* cannot be modified.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

**PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

**Note:** You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the *selang authorize* command to add programs, accessors, and their access types to a PACL. You can use the *authorize-* command to remove accessors from a PACL.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the *audit* parameter of the *chres* and *chfile* commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

**Note:** The SECLABEL property corresponds to the *label[-]* parameter of the *chres* and *ch[x]usr* commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the *level[-]* parameter of the *ch[x]usr* and *chres* commands.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the *defaccess* parameter with the *chres*, *editres*, or *newres* command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.



## PROGRAM Class

Each record in the PROGRAM class defines a program that is considered part of the trusted computing base. Programs in this class are trusted not to have security breaches because they are monitored by the Watchdog to ensure that they are not modified. If a trusted program is altered, Privileged Access Manager automatically marks the program as untrusted, and the program is prevented from executing. Optionally, you can also allow or prevent execution of untrusted programs using the BLOCKRUN property.

Each PROGRAM record contains several properties that define information about the trusted program file.

Usage notes:

- On UNIX, the PROGRAM class can also contain programs that are not marked as setuid or setgid.
- You can define any program as a trusted program within Privileged Access Manager.  
A program cannot be used in a program access control list (PACL) unless it is defined in the PROGRAM class. (However, a program is automatically added to the PROGRAM class when it is added to a PACL.)
- Directories cannot be defined in the PROGRAM class.

The key of the PROGRAM class record is the file name of the program the record protects. Specify the full path of the file as the objectname.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Properties marked *informational* cannot be modified.

- **ACCSTIME**  
(Informational). The date and time the record was last accessed.
- **ACCSWHO**  
(Informational). The administrator who last accessed the record.
- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the access types of the accessor. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the authorize or authorize- command to modify the ACL.
- **BLOCKRUN**  
Specifies whether to check if the program is trusted and blocks the execution of untrusted programs. The execution blocking is performed regardless whether the program is a setuid or a regular program.  
Use the blockrun[-] parameter with the chres, editres, and newres commands to modify this property for resources.
- **CATEGORY**  
Defines one or more security categories that are assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record. Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **MD5**  
(Informational). The RSA-MD5 signature of the file.
- **NACL**

The NACL property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**  
Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **OWNER**

Defines the user or group that owns the record.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the via(*pgm*) parameter with the selang authorize command to add programs, accessors, and their access types to a PACL. You can use the authorize- command to remove accessors from a PACL.

#### **NOTE**

For resources in PROGRAM class, PACL applies only to setuid/setgid programs on UNIX or programs with *file* resource on Windows. Privileged Access Manager first checks for the file resource record, and if the access is allowed, then it checks the program resource record.

#### **PGMINFO**

Defines the program information that is automatically generated by Privileged Access Manager.

The Watchdog automatically verifies the information that is stored in this property. If it is changed, Privileged Access Manager defines the program as untrusted.

You can select any of the following flags to *exclude* the associated information from this verification process:

- **crc**  
The cyclic redundancy check and MD5 signature.
- **ctime**  
(UNIX only) The time of the last file status change.
- **device**  
On UNIX, the logical disk that the file resides on. On Windows, the drive number of the disk containing the file.
- **group**  
The group that owns the program file.
- **inode**  
On UNIX, the file system address of the program file. On Windows, this flag has no meaning
- **mode**  
The associated security protection mode for the program file.
- **mtime**  
The time the program file was last modified.
- **owner**  
The user who owns the program file.
- **sha1, sha256, sha384, sha512**  
The SHA1, SHA256, SHA384, or SHA512 signature. Digital signature method called Secure Hash Algorithm that could be applied to the program or sensitive files.
- **size**  
The size of the program file.

Use the flags, flags+, or flags- parameter with the chres, editres, or newres command to modify the flags in this property.

## RAUDIT

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## SECLABEL

Defines the security label of a user or resource.

### NOTE

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## SECLEVEL

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

### **UNTRUST**

Defines whether the resource is untrusted or trusted. If the UNTRUST property is set, accessors cannot use the resource. If the UNTRUST property is not set, the other properties listed in the database for the resource are used to determine accessor's access authority. If a trusted resource is changed in any way, Privileged Access Manager automatically sets the UNTRUST property.

Use the trust[-] parameter with the chres, editres, or newres command to modify this property.

### **UNTRUSTREASON**

(Informational). The reason why the program became untrusted.

### **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

### **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

### **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted. If an access request violates an access rule, a record is written to the audit log.

## **PWPOLICY Class**

Each record in the PWPOLICY class defines a password policy. These policies are sets of rules for both the validity of new passwords, and for the length of time the passwords are valid.

The key to the PWPOLICY class is the name of the password policy.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **APPLS**

(Informational). The list of CA SSO applications that are linked to the password policy.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **OWNER**

Defines the user or group that owns the record.

- **PASSWDRULES**

Specifies the password rules. This property contains a number of fields that determine how Privileged Access Manager handles password protection. For a complete list of the rules, see the modifiable property PROFILE of the USER class.

Use the `passwordparameter` and the `rules` or `rules-` option with the `setoptions` command to modify this property.

- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## REGKEY Class

### Valid on Windows

Each record in the REGKEY class defines a key in the Windows registry.

The key to a REGKEY record is the full registry path to the key.

#### NOTE

You can use wildcard characters as part of the path specification.

By default Privileged Access Manager protects the Privileged Access Manager registry entries. The root of this registry entry is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
```

Privileged Access Manager also protects the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

The REGKEY class and the REGVAL class have identical properties. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

#### NOTE

HKLM/CurrentControlSet is a reference to ControlSet001 which Privileged Access Manager does not monitor. Point REGKEY / REGVAL resources to ControlSet001 instead of CurrentControlSet.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also *ACL*, *CALACL*, *PACL*. Each entry in the *NACL* contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

**PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (*PACL*) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the *PROGRAM* class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a *PACL*.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a *PACL*. You can use the `authorize-` command to remove accessors from a *PACL*.

**RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. *RAUDIT* derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## REGVAL Class

### Valid on Windows

Each record in the REGVAL class defines a value in the Windows registry

The key to a REGVAL record is the full registry path to the value.

**Note:** You can use wildcard characters as part of the path specification.

**Note:** The REGVAL class allows the following access types: NONE, READ, WRITE, DELETE.

The REGVAL class and the REGKEY class have identical properties. These properties are as follows. (Non-modifiable properties are marked *informational*.)

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the authorize or authorize- command to modify the ACL.

- **COMMENT**

Defines additional information that you want to include in the record. The product does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also *ACL*, *CALACL*, *PACL*. Each entry in the *NACL* contains the following information:

**Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

**NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. The product can email the audit record to the specified user.

**Limit:** 30 characters.

**OWNER**

Defines the user or group that owns the record.

**PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (*PACL*) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the *PROGRAM* class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

**Note:** You can use wildcard characters to specify the resource in a *PACL*.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a *PACL*. You can use the `authorize-` command to remove accessors from a *PACL*.

**RAUDIT**

Defines the types of access events that the product records in the audit log. *RAUDIT* derives its name from *Resource AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

The product records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.



Use the audit parameter of the chres and chfile commands to modify the audit mode.

## UACC

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to the product or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

## UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

## WARNING

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## RESOURCE\_DESC Class

Each record in the RESOURCE\_DESC class defines all of the names that new user-defined class objects are allowed to access in CA SSO. You cannot create a new object in the RESOURCE\_DESC class; you can only modify the existing ones.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **CLASS\_RIGHT**  
Of the 32 optional access rights; all are modifiable. The defaults for the first four rights are:
  - CLASS\_RIGHT1-read
  - CLASS\_RIGHT2-write
  - CLASS\_RIGHT3-execute
  - CLASS\_RIGHT4-rename
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **OWNER**  
Defines the user or group that owns the record.
- **RESPONSE\_LIST**  
The name of the object in the RESPONSE\_TAB class that contains this object's name.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## RESPONSE\_TAB Class

Each record in the RESPONSE\_TAB class defines a CA SSO response table to different authorization decisions.

A response is a personalized answer that is returned to application after an authorization request is granted or denied. It consists of KEY=VALUE pairs that are understood by the specific application. The response provides the ability to personalize the portal site according to the user's specific needs and authorization permissions.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using *selang* or the administration interfaces. Non-modifiable properties are marked *informational*.

- **CLASS\_RIGHT**  
32 optional response properties are lists of strings containing KEY=VALUE pairs (for example, button1=yes, picture2=no, and so on). There should be one property for each access value.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **OF\_RESOURCE**  
The name of the object in the RESOURCE\_DESC class that refers to the same user-defined class.
- **OWNER**  
Defines the user or group that owns the record.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## RULESET Class

Each record in the RULESET class represents a set of rules which define a policy.

The key of the RULESET class record is the name of the policy the record is linked to.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using *selang* or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**  
Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the access authority that the accessor has to the resource.
 Use the access parameter with the *authorize* or *authorize-* command to modify the ACL.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the *chres*, *ch[x]usr*, or *ch[x]grp* commands to modify this property.

The resolution of daytime restrictions is one minute.

- **EXPANDED COMMANDS**

(Informational) Displays the variable values of the commands in the deployed policy.

- **EXPANDED UNDO COMMANDS**

(Informational) Displays the variable values of the undo commands in the deployed policy.

- **FINALIZE**

Specifies whether the selang scripts have been finalized (and hence the policy version can be deployed).

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

#### **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

#### **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

#### **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

#### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the selang authorize command to add programs, accessors, and their access types to a PACL. You can use the authorize- command to remove accessors from a PACL.

#### **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

## **RULESET\_DOCMD\_IDX**

(Informational). The command index; that is, a counter of the number of commands in the list of RULESET\_DOCMDS.

## **RULESET\_DOCMDS**

The list of selang commands which, together, define the policy. These are the commands that are executed to deploy the policy.

### **WARNING**

Policy deployment does not support commands that set user passwords. Do not include such commands in your deployment script file. UNIX (native) selang commands are supported but will not show in deviation reports.

## **RULESET\_POLICIES**

(Informational). The list of policies (POLICY objects) that use this set of rules.

## **RULESET\_UNDOCMD\_IDX**

(Informational). The command index; that is, a counter of the number of commands in the list of RULESET\_UNDOCMDS.

## **RULESET\_UNDOCMDS**

The list of selang commands which, together, define the policy undeployment script. These are the commands that are executed to undeploy the policy.

## **SECLABEL**

Defines the security label of a user or resource.

### **NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

## **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

## **SIGNATURE**

A hash value based on the RULESET\_DOCMDS and RULESET\_UNDOCMDS properties.

## **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

## **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

## **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## **SECFILE Class**

Each record in the SECFILE class defines a file to be monitored. SECFILE class records provide verification for important files in the system. However, they cannot appear in a conditional access control list.

Add sensitive system files that are not frequently modified to this class to verify that an unauthorized user has not altered them. The following are some examples of the type of files to include in class SECFILE:

For UNIX	For Windows
/.rhosts	\system32\drivers\etc\hosts
/etc/services	\system32\drivers\etc\services
/etc/protocols	\system32\drivers\etc\protocols
/etc/hosts	
/etc/hosts.equiv	

The Watchdog scans these files and ensures the information known about these files is not modified.

### **NOTE**

Directories cannot be defined in the SECFILE class.

The key of the SECFILE class record is the name of the file that the SECFILE record protects. Specify the full path.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **AIXACL**  
AIX system ACLs.
- **AICEXTI**  
AIX system extended information.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **GROUPS**  
Defines the list of CONTAINER records that a resource record belongs to.  
To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.  
Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.
- **HPUXACL**  
HP-UX system ACLs.
- **MD5**  
(Informational). The RSA-MD5 signature of the file.
- **OWNER**  
Defines the user or group that owns the record.
- **PGMINFO**

Defines the program information automatically generated by Privileged Access Manager.

The Watchdog automatically verifies the information stored in this property. If it is changed, Privileged Access Manager defines the program as untrusted.

You can select any of the following flags to *exclude* the associated information from this verification process:

- **crc**  
The cyclic redundancy check and MD5 signature.
- **ctime**  
(UNIX only) The time of the last file status change.
- **device**  
On UNIX, the logical disk that the file resides on. On Windows, the drive number of the disk containing the file.
- **group**  
The group that owns the program file.
- **inode**  
On UNIX, the file system address of the program file. On Windows, this has no meaning
- **mode**  
The associated security protection mode for the program file.
- **mtime**  
The time the program file was last modified.
- **owner**  
The user who owns the program file.
- **sha1**  
The SHA1 signature. Digital signature method called Secure Hash Algorithm that could be applied to the program or sensitive files.
- **size**  
The size of the program file.

Use the flags, flags+, or flags- parameter with the chres, editres, or newres command to modify the flags in this property.

- **UNTRUST**

Defines whether the resource is untrusted or trusted. If the UNTRUST property is set, accessors cannot use the resource. If the UNTRUST property is not set, the other properties listed in the database for the resource are used to determine accessor's access authority. If a trusted resource is changed in any way, Privileged Access Manager automatically sets the UNTRUST property.

Use the trust[-] parameter with the chres, editres, or newres command to modify this property.

**Note:** The resource file is used to determine access authority, when the SECFILE resource is untrusted and no access authority is set to the SECFILE resource.

- **UNTRUSTREASON**

(Informational). The reason why the program became untrusted.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## SECLABEL Class

Each record in the SECLABEL class associates a security level with security categories. A security label overrides the specific security level and security category assignments in the USER record if the SECLABEL class is active. Assigning a security label is equivalent to explicitly assigning the security level and security categories of the security label to the user.

When a USER record includes a security label, the user is granted access to a resource only if the following conditions are met:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

#### **NOTE**

On Windows, each security label defined to Privileged Access Manager must have a record in the SECLABEL class.

The key of the SECLABEL class record is the name of the security label. This name is used to identify the security label when assigning it to a user or resource.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **OWNER**  
Defines the user or group that owns the record.
- **SECLEVEL**  
Defines the security level of an accessor or resource.  
**Note:** This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## **SEOS Class**

The SEOS class controls the behavior of the Privileged Access Manager authorization system.

The class contains only one record, called SEOS, which specifies general security and authorization options. To view or change the status of SEOS class properties, use the `setoptions` command.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACCPACL**  
Indicates the order in which the UACC (`defaccess`) and PACL lists are scanned during authorization.  
When ACCPACL is active and explicit access is provided for a user through an ACL, then that accessor is the allowed access. If there is no explicit access through an ACL but explicit access is defined through a PACL, then the PACL access is the allowed access. If neither ACL or PACL contains explicit access, `defaccess` is checked for access definitions.  
If ACCPACL is not activated, the ACL is still checked first for explicit access. If the ACL contains no explicit access definitions for the resource being checked, `defaccess` definitions are checked next. If no explicit access is defined in `defaccess`, then the PACL access definitions are checked.  
When Privileged Access Manager is installed, the value of this property is set to yes.  
Use the `accpac` or `accpac-` parameter with the `setoptions` command to modify this property.
- **ADMIN**

Each record in the ADMIN class defines what authorization privileges non-admin users have to administer specific classes. Each Privileged Access Manager class that is to be administered by specific non-admin users is represented by an ADMIN record. The record contains a list of accessors with the access authority of each.

Example: To allow user John to view FILE class rules, specify "authorize ADMIN FILE uid(John) access(read)"

If ADMIN class is off, then a non-admin user cannot get administrator privileges using this ADMIN class.

- **APPL**  
Indicates whether the APPL class is active.
- **AUTHHOST**  
Indicates whether the AUTHHOST class is active.
- **CALENDAR**  
Indicates whether the CALENDAR class is active.
- **CATEGORY**  
Indicates whether the CATEGORY class is active.
- **CNG\_ADMIN\_PWD**  
Indicates whether a user with the PWMANAGER attribute can change an ADMIN user password using selang. The default is yes.  
Use the class+ or class- parameter and the *cng\_adminpwd* option with the setoptions command to activate or inactivate this property.
- **CNG\_OWN\_PWD**  
Indicates whether users can change their own passwords using selang.  
Use the class+ or class- parameter and the *cng\_ownpwd* option with the setoptions command to activate or inactivate this property.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CONNECT**  
Indicates whether the CONNECT class is active. When the CONNECT class is active, records in the class protect the outgoing connections.  
If the HOST class is active, the CONNECT class is not used as an active class, even when activated.  
If the TCP class is active, the CONNECT class is not used as an active class.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIMERES**  
(UNIX only) Indicates whether Privileged Access Manager checks the daytime restrictions on resources.
- **DMS**  
List of DMS servers this database should send notifications to.
- **DOMAIN**  
(Windows only) Indicates whether the DOMAIN class is active.
- **ENDTIME**  
(Informational). The date and time the database files were last closed in an orderly manner.
- **FILE**  
Indicates whether the FILE class is active. When the FILE class is active, records in the class protect files and directories.
- **ACCGRR**

The *accumulative group rights* option (ACCGRR) affects how Privileged Access Manager checks the ACL of a resource. If ACCGRR is enabled, Privileged Access Manager checks the ACL for the authorities that are granted from all the groups to which the user belongs. If ACCGRR is disabled, Privileged Access Manager checks the ACL to see if any of the applicable entries contain the value none. If so, access is denied. Otherwise Privileged Access Manager ignores all group



entries except the first applicable one in the access control list. Use the command setoptions ACCGRR command to enable or disable this property.

- **HOLIDAY**  
Indicates whether the HOLIDAY class is active. When the HOLIDAY class is active, users need extra permission to log in during defined Holiday periods.
- **HOST**  
Indicates whether the HOST class is active. When the HOST class is active, Privileged Access Manager protects incoming TCP/IP service requests from remote hosts.  
If the HOST class is active, the TCP and CONNECT classes are not used as active classes, even when activated. The default for the HOST class is active.
- **INACT**  
Indicates the number of inactive days after which user login is suspended. An inactive day is a day in which the user does not log in.  
A value for the INACTIVE property in a USER record overrides a value in a GROUP record. Both override the INACT property in the SEOS class record.  
Use the inactive or inactive- parameter with the setoptions command to update this property.
- **ISDMS**  
True if the PMDB serves as a DMS.
- **LOGINAPPL**  
(UNIX only) Indicates whether the LOGINAPPL class is active.
- **MAXLOGINS**  
The maximum number of concurrent logins (terminal sessions) a user is allowed, after which the user is denied access. A zero value indicates no maximum and the user can log in to any number of terminal sessions concurrently. The value must be either zero or greater than 1 if the user wants to log in and run selang or otherwise administer the database, because Privileged Access Manager considers each task (login, selang, GUI, and so forth) to be a terminal session.  
A value for the MAXLOGINS property in a USER record overrides a value in a GROUP record. Both override the MAXLOGINS property in the SEOS class record. The value in the SEOS record is the default value used when there is no explicit value in the accessor record.  
Use the maxlogins parameter with the chres, editres, and newres commands to modify this property for the SEOS class.
- **MFTERMINAL**  
Indicates whether the MFTERMINAL class is active.
- **PASSWDRULES**  
Indicates the password rules. This property contains a number of fields that determine how Privileged Access Manager handles password protection. For a complete list of the rules, see the modifiable property PROFILE of the USER class. Use the passwordparameter and the rules or rules- option with the setoptions command to modify this property.
- **PASSWORD**  
Indicates whether password checking is active.  
Use the class+ or class- parameter and the PASSWORD option with the setoptions command to activate or inactivate this property.
- **PROCESS**  
Indicates whether the PROCESS class is active. When the PROCESS class is active, records in the class protect defined processes from kill attempts.  
The file must also be defined in the FILE class.
- **PROGRAM**  
Indicates whether the PROGRAM class is active. When the PROGRAM class is active, records in the class protect defined programs that were marked as Trusted.
- **PWPOLICY**  
Indicates whether the PWPOLICY class is active.
- **REGKEY**

- (Windows only) Indicates whether the REGKEY class is active.
- **REGVAL**  
(Windows only) Indicates whether the REGVAL class is active.
- **RESOURCE\_DESC**  
Indicates whether the RESOURCE\_DESC class is active.
- **RESPONSE\_TAB**  
Indicates whether the RESPONSE\_TAB class is active.
- **SECLABEL**  
Indicates whether the SECLABEL class is active.
- **SECLEVEL**  
Indicates whether the SECLEVEL class is active.
- **STARTTIME**  
(Informational). The date and time the database files were last opened.
- **SUDO**  
Indicates whether the SUDO class, used by sesudo, is active.
- **SYSTEM\_AAUDIT\_MODE**  
Specifies the default audit mode (systemwide audit mode) for users and enterprise users.  
**Default:** Failure LoginSuccess LoginFailure
- **SURROGATE**  
Indicates whether the SURROGATE class is active. When the SURROGATE class is active, Privileged Access Manager protects surrogate requests.
- **TCP**  
Indicates whether the TCP class is active. When the TCP class is active, Privileged Access Manager protects incoming and outgoing TCP services such as mail, ftp, and http.  
If the HOST class is active, the TCP class is not used as an active class, even when activated.  
If the TCP class is active, the CONNECT class is not used as an active class.
- **TERMINAL**  
Indicates whether the TERMINAL class is active. When the TERMINAL class is active, Privileged Access Manager performs a terminal access check during sign-on and protects X-window sessions.
- **USER\_ATTR**  
Indicates whether the USER\_ATTR class is active.
- **USER\_DIR**  
Indicates whether the USER\_DIR class is active.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## SPECIALPGM Class

The SPECIALPGM class gives specified programs special security privileges.

Each record in the SPECIALPGM class has one of two functions:

- Registering backup, DCM, PBF, PBN, STOP, SURROGATE, REGISTRY, and KILL programs in Windows or registering xdm, backup, mail, DCM, PBF, PBN, stop, and surrogate programs in UNIX.
- Associating an application that needs special Privileged Access Manager authorization protection with a logical user ID. This effectively allows setting access permissions according to *what* is being done rather than *who* is doing it.

### NOTE

When defining a program in the SPECIALPGM class, we recommend that you also define it in the FILE class. The FILE resource protects the executable by preventing someone from modifying (replacing or corrupting) the

executable without authorization, and the PROGRAM resource verifies that the program does not run if it was modified when Privileged Access Manager was not running.

**NOTE**

You cannot define a record in the SPECIALPGM class for incoming network interception events. This is because the incoming network interception event does not have a process name in this context. To bypass writing an audit record for the interception event, set the AUDIT property to NONE for the corresponding record in the TCP class

Use the PGMTYPE property to register system services, daemons, or other special programs.

Use the SEOSUID and NATIVEUID properties to assign a logical user to a program.

The key of the SPECIALPGM class record is a path to the special program or to a range, or pattern, of special programs.

**NOTE**

The maximum number of rules that you can place in the specialpgm class table is 512.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non modifiable properties are marked *informational*.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **NATIVEUID**

Indicates the user invoking the program or process. Use \* to specify all Privileged Access Manager users.

Use the nativeuid parameter with the chres, editres, or newres command to modify this property.

**NOTE**

For backward compatibility with older versions of Privileged Access Manager, you can use the UNIXUID property instead of the NATIVEUID property.

- **OWNER**

Defines the user or group that owns the record.

- **PGMTYPE**

Determines the types of access checks that Privileged Access Manager bypasses when granting access.

- **backup**

Bypasses READ, CHDIR, and UTIME access.

**NOTE**

There are two ways to run a successful backup. If the backup program is executed by a non-root user, you have to define this user as an OPERATOR. If the backup program is executed by root, it is enough to register the backup program in the SPECIALPGM class as pgmtype(backup).

- **changeid**

(UNIX only) Bypass all the change identity tools except for the PAM enabled surrogate tool.

**NOTE**

For example: er specialpgm /bin/mail pgmtype(changeid)

- **dcm**

(Windows) Bypasses all security checks for all events except STOP events.

(UNIX) Bypasses security checks for READ and EXEC events.

- **fullbypass**

Fully bypasses all Privileged Access Manager authorization and database checks. Privileged Access Manager ignores a process that has this property, and no record of any process events appears in audit, trace, or debug logs.

- **kill**

(Windows only) Bypasses program termination for a process.

For example, the following rule provides a bypass to the services.exe if this process tries to open handles to Privileged Access Manager services (processes) with access mask KILL:

```
nr specialpgm c:\Windows\system32\services.exe pgmtype(kill)
```

On Windows Server 2008, the services.exe process, which manages the stopping and starting of services, opens handles to Privileged Access Manager services (processes) with access type KILL to manage process termination and startup. During installation on Windows Server 2008, Privileged Access Manager runs a discovery process to locate services.exe and creates a bypass rule for it. Without this bypass, you receive DENIED Privileged Access Manager audit events when services.exe is trying to open handles of Privileged Access Manager services.

- **mail**  
(UNIX only) Bypasses database checks for setuid and setgid events. The mail bypass allows you to trace mail access attempts.
- **none**  
Removes any PGMTYPE previously set.
- **pbf**  
Bypasses database checks for file handling events.
- **pbn**  
Bypasses database checks for network-related events.
- **propagate**  
Propagates its own security privileges to any programs that are called from a program with this PGMTYPE. If you do not specify this, SPECIALPGM privileges only affect the parent program. SPGM batch files, including propagate, are supported for executables only.

#### NOTE

Security privilege propagation works with PBF, PBN, DCM, FULLBYPASS, and SURROGATE privileges only.

### registry

(Windows only) Bypasses database checks for programs that manipulate the Windows registry.

- **stop**  
Bypasses database checks for the STOP feature.
- **surrogate**  
Bypasses database checks for identity changing events in the kernel. You cannot trace if you use the surrogate bypass.
- **xm**  
(UNIX only) Bypasses network events (such as TCP, HOST, and CONNECT classes) for a limited network range (6000-6010).

Use the pgmtype parameter with the chres, editres, or newres command to modify this property.

### SEOSUID

Defines the surrogate logical user authorized to run this special program. This logical user must be defined in the database with a USER record.

Use the seosuid parameter with the chres, editres, or newres command to modify this property.

### UPDATE\_TIME

(Informational) Displays the date and time when the record was last modified.

### UPDATE\_WHO

(Informational) Displays the administrator who performed the update.

### Example: Protect a UNIX file

To protect a file that resides in `/DATABASE/data/*`, the Database Manager uses a file server daemon named `firmdb_filemgr`. This file server resides on `/opt/dbfirm/bin/firmdb_filemgr`. This daemon usually runs under root, making the data accessible to any root-shell hack.

In the following example, the logical user is defined as the only accessor of these files; access by others is restricted:

1. Define the sensitive files to Privileged Access Manager using the command:

```
newres file /DATABASE/data/* defaccess(NONE) owner(nobody)
```

2. Define the logical user to access the files:

```
newusr firmDB_mgr
```

3. Allow only the logical user `firmDB_mgr` to access the files.

```
authorize file /DATABASE/data/* uid(firmDB_mgr) access(ALL)
```

4. Finally, make `firmdb_filemgr` run with logical user `firmDB_mgr`

```
newres SPECIALPGM /opt/dbfirm/bin/firmdb_filemgr unixuid(root) \
seosuid(firmDB_mgr)
```

Consequently, when the daemon accesses the files, Privileged Access Manager recognizes the logical user as the accessor of the files, and not root. A hacker who attempts to access the files as root does not succeed.

### Example: Protect a Windows file

To protect files that reside in `C:\DATABASE\data`, the Database Manager uses a file server service named `firmdb_filemgr.exe`. This file server resides on `C:\Program Files\dbfirm\bin\firmdb_filemgr.exe`. This service usually runs under the system account, making the data accessible to any system hack.

In the following example, the logical user is defined as the only accessor of these files; access by others is restricted:

1. Define the sensitive files to Privileged Access Manager using the following command:

```
newres file C:\DATABASE\data\* defaccess(NONE) owner(nobody)
```

2. Define a logical user to access the files:

```
newusr firmDB_mgr
```

3. Allow only the logical user `firmDB_mgr` to access the files:

```
authorize file C:\DATABASE\data\* uid(firmDB_mgr) access(ALL)
```

4. Finally, make `firmdb_filemgr` run with logical user `firmDB_mgr`:

```
newres SPECIALPGM ("C:\Program Files\dbfirm\bin\firmdb_filemgr.exe") \
nativeuid(system) seosuid(firmDB_mgr)
```

Consequently, when the service accesses the files, Privileged Access Manager recognizes the logical user as the accessor of the files, and not the system account. A hacker who attempts to access the files in the system account does not succeed.

## SUDO Class

Each record in the SUDO class identifies a command for which a user can borrow permissions from another user using the `sesudo` command.

The key of the SUDO class record is the name of the SUDO record. This name is used instead of the command name when a user executes the commands in the SUDO record.

### NOTE

If you create a SUDO record for an interactive Windows application, you must set the interactive flag for the SUDO record. If you do not set the interactive flag, the application runs in the background and you cannot interact with it. For more information, see the *Troubleshooting Guide*.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

The command that `sesudo` executes.

The alphanumeric string can contain up to 255 characters, which include the command and also permitted and prohibited parameters.

For example, the following profile definition uses the **COMMENT** property properly:

```
newres SUDO profile_name comment('command;;NAME')
```

**NOTE**

This use of the **COMMENT** property is different than in other classes. For more information about defining SUDO records, see the *Endpoint Administration Guide* for your OS. This property was also known as **DATA** in earlier versions of Privileged Access Manager.

**Limit:** 255 characters.

Use the `comment[-]` parameter with the `chres`, `editres`, and `newres` commands to modify this property.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the `restrictions` parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

The list of GSUDO or CONTAINER records a resource record belongs to.

To modify this property in a SUDO class record, you must change the **MEMBERS** property in the appropriate CONTAINER or GSUDO record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **INTERACTIVE**

(Windows only). This switch should be marked when the application you intend to run via `sesudo` is an interactive Windows application (for example, `notepad.exe` or `cmd.exe`) and not a service application. If you are trying to run an interactive application using `sesudo` that is not marked as *interactive*, the application runs in the background without the ability to interact with it.

**NOTE**

Some Windows applications can not run in the foreground because of a Windows limitation.

- **NACL**

The **NACL** property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, `write`). See also **ACL**, **CALACL**, **PACL**. Each entry in the **NACL** contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

- **OWNER**

Defines the user or group that owns the record.

## **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- – **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

### **NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

- **PASSWORDREQ**

(UNIX only) Indicates whether the `sesudo` command requests the original user's password before executing.

Use the `password` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **POLICYMODEL**

Specifies the PMDB that receives new passwords when you change user passwords with the `sepass` utility. The passwords are *not* sent to the Policy Model defined by the `parent_pmd` or `passwd_pmd` configuration settings if a value is entered for this property.

**Note:** This property corresponds to the `pmdb[-]` parameter of the `ch[x]usr` and `ch[x]grp` commands.

- **SECLABEL**

Defines the security label of a user or resource.

### **NOTE**

The SECLABEL property corresponds to the `label[-]` parameter of the `chres` and `ch[x]usr` commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.

- **TARGUSR**

(UNIX only) Indicates the target uid, which identifies the user whose permissions are to be borrowed for executing the command. The default is `root`.

Use the `targuid` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## **SURROGATE Class**

Each record in the SURROGATE class defines restrictions that protect a user from other users when they try to change their identity to his or hers. Privileged Access Manager treats a change identity request as an abstract object that can be accessed only by authorized users.

A record in the SURROGATE class represents each user or group who has surrogate protection. Two special records-USER.\_default and GROUP.\_default-represent users and groups who do not have individual SURROGATE records. If there is no need to differentiate between the default for users and the default for groups, you may use the \_default record for the SURROGATE class instead.

### **NOTE**

Many Windows utilities and services (for example, Run As) identify as user *NT AUTHORITY\SYSTEM* and not as the original user running them. To let users who use these utilities and services as impersonate another user, you must create this SYSTEM user in the Privileged Access Manager database and authorize it to impersonate the target user.

The key of the SURROGATE class record is the name of the SURROGATE record.

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors access types.

Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the authorize or authorize- command to modify the ACL.

- **CALACL**

Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the Unicenter NSM calendar status.

Each element in the calendar access control list (CALACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Calendar**



Defines a reference to a calendar in Unicenter TNG.

- **Access**

Defines the access authority that the accessor has to the resource.

Access is permitted only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the access defined in the calendar ACL.

- **CALENDAR**

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in Privileged Access Manager. Privileged Access Manager fetches Unicenter TNG active calendars at specified time intervals.

- **CATEGORY**

Defines one or more security categories that are assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

- **OWNER**

Defines the user or group that owns the record.

- **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Program**

Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.

- **Access**

Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.
- Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the `label[-]` parameter of the `chres` and `ch[x]usr` commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**NOTE**

This property corresponds to the `level[-]` parameter of the `ch[x]usr` and `chres` commands.

- **UACC**

Defines the default access authority for the resource, which indicates the access that is granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example 1:** An example to show how the SURROGATE rule refrains user “john” from switching to the “root” user to perform privileged operations.

**Step 1:** Create a user “john”.

```
PAMSC> nu john pass(john)
```

**Step 2:** Write the SURROGATE rule to protect “root” from the user “John”.

```
PAMSC> er SURROGATE USER.root owner(root) defacc(r)
```

```
PAMSC> auth SURROGATE USER.root uid(john) access(n)
```

**Step 3:** Verify if “john” can switch to root using “su”.

The SURROGATE rule restricts “john” from switching to the “root” account.

**Example 2:** An example to show how the SURROGATE rule refrains user “smith” from switching to another user “john”.

**Step 1:** Create a user “smith”.

```
PAMSC> nu smith pass(smith)
```

**Step 2:** Create a user “john”.

```
PAMSC> nu john pass(john)
```

**Step 3:** Write a SURROGATE rule to protect “john” from “smith”.

```
PAMSC> er SURROGATE USER.john owner(john) defacc(r)
```

```
PAMSC> auth SURROGATE USER.john uid(smith) access(n)
```

**Step 4:** Verify if “smith” can switch to “john” using “su”.

The SURROGATE rule restricts “smith” from switching to the “john” account.

**Example 3:** An example to protect user groups using SURROGATE rule.

**Step 1:** Create a group “finance”.

```
PAMSC> ng finance unix
```

**Step 2:** Create a group “engineering”.

```
PAMSC> ng engineering unix
```

**Step 3:** Create a user “john” and join the user to the 'finance' group.

```
PAMSC> nu john pass(john)
```

```
PAMSC> eu john unix pgroup(finance)
```

**Step 4:** Create a user “smith” and join the user to the 'engineering' group.

```
PAMSC> nu smith pass(smith)
```

```
PAMSC> eu smith unix pgroup(engineering)
```

**Step 5:** Prevent users from “engineering” to switch to users in “finance” group.

```
PAMSC> er SURROGATE GROUP.finance defacc(r)
```

```
PAMSC> auth SURROGATE GROUP.finance gid(engineering) access(n)
```

**Step 6:** Log in as “smith” user from “engineering” and try to switch to the user “john” from the “finance” group. You notice that the access is denied due to the SURROGATE rule.

The ideal way to implement SURROGATE policy in an enterprise is to create SURROGATE rule with access via PROGRAM /opt/CA/PAMSC/bin/sesu.

The original 'su' program is backed up in a separate place and made as a link to /opt/CA/PAMSC/bin/sesu. This way, we force users to switch to other account only via 'sesu' PROGRAM. With this implementation, the example 1 changes as follows wherein we allow all users to switch to 'root' via 'sesu' PROGRAM and specifically deny access to the user "john" from switching to root.

```
PAMSC> SURROGATE USER.root owner(root) defacc(n)
```

```
PAMSC> auth SURROGATE USER.root uid(*) via(pgm(/opt/CA/PAMSC/bin/sesu))
```

```
PAMSC> auth SURROGATE USER.root uid(john) access(n)
```

## TCP Class

Each record in the TCP class defines a TCP/IP service such as mail, ftp, and http. When the TCP class is being used for authorization, hosts can obtain services from the local host only if the TCP resources grant access. Also, users or groups on a local host can use the TCP/IP services to access remote hosts only if the TCP resources grant access.

The ACL in a TCP record can specify access types for hosts (HOST), groups of hosts (GHOST), networks (HOSTNET), and sets of hosts (HOSTNP).

The CACL in a TCP record can specify access types for hosts (HOST), groups of hosts (GHOST), networks (HOSTNET), and sets of hosts (HOSTNP), and can also specify access types for users and groups.

You can set rules based on IPv4 or IPv6 addresses, not just on host names. This means that you can cater for a domain name change.

The key of the TCP record is the name of the TCP/IP service. The TCP class controls both outgoing services and incoming services.

The following definitions describe the properties contained in a TCP class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines the hosts for which the local host provides service and the access types that are allowed.

Each element in the access control list contains the following information:

- **Host reference**

Defines a HOST, GHOST, HOSTNET, or HOSTNP record.

- **Permitted access**

The access authority that the referenced host has to the resource. The valid access authorities are:

- **none** Does not allow the host to perform any operations.
- **read** Allows the host to obtain TCP service from the local host.

Use the access parameter of the authorize or authorize- command to modify this property

- **CACL**

A list of accessors (users and groups) permitted to access the resource and the host or hosts they can access. Each element in the conditional access control list (CACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Host reference**

Defines a HOST, GHOST, HOSTNET, or HOSTNP record

- **Access** Defines the access authority that the accessor has to the resource. The valid access types are:

- **write** Allows the accessor to use this service to access the host or group of hosts.
- **none** Does not allow the accessor to use this service to access the host or group of hosts.

Use the authorize or authorize- command to modify this property.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the authorize deniedaccess command, or the authorize- deniedaccess- command, to modify this property.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

- **OWNER**

Defines the user or group that owns the record.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**
- No access requests. Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

- **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

**Example 1:** Prevent incoming connections from a remote host by using Telnet.

**Step 1:** Disable HOST and CONNECT classes, and enable TCP class.

```
PAMSC> so class-(HOST)
PAMSC> so class-(CONNECT)
PAMSC> so class+(TCP)
```

**Step 2:** Add a remote host ([My\\_Remote\\_Host.example.com](#)) in /etc/hosts. Run the following command at the command prompt.

```
vi /etc/hosts
```

**Step 3:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildla -h
```

**Step 4:** Run the following command at the command prompt to verify that the remote host ([My\\_Remote\\_Host.example.com](#)) is added to /etc/hosts.

```
./sebuildla -H
```

**Step 5:** Define a remote host ([My\\_Remote\\_Host.example.com](#)) from which we prevent incoming Telnet connections.

```
PAMSC> nr HOST My\_Remote\_Host.example.com
```

**Step 6:** Define a TCP resource for the Telnet service which allows outgoing Telnet connections.

```
PAMSC> nr TCP telnet owner(nobody) defaccess(w)
```

**Step 7:** Set a rule that prevents incoming connections from the remote host ([My\\_Remote\\_Host.example.com](#)) by using Telnet.

```
PAMSC> authorize TCP telnet HOST(My\_Remote\_Host.example.com) access(n)
```

**Step 8:** Try connecting from the remote host to the Privileged Access Manager endpoint by using Telnet. The connection fails but other connections are not affected.

**Example 2:** Prevent a user from accessing all remote hosts by using Telnet service.

**Step 1:** Disable HOST and CONNECT classes, and enable TCP class.

```
PAMSC> so class-(HOST)
PAMSC> so class-(CONNECT)
PAMSC> so class+(TCP)
```

**Step 2:** Execute the following command at the command prompt and add all remote hosts to /etc/hosts.

```
vi /etc/hosts
```

**Step 3:** For network interception, the lookahead database "ladb" must be properly entered with the remote host address. To ensure this works, run the following command at the command prompt.

```
./sebuildla -h
```

**Step 4:** Define remote hosts as resources by creating a host name pattern that covers all the remote hosts.

```
PAMSC> nr HOSTNP *
```

**Step 5:** Set a rule that denies a user (john) from accessing all the remote hosts.

```
PAMSC> auth TCP telnet uid(john) hostnp(*) access(n)
```

**Step 6:** Log in as john and try to access any remote host by using Telnet. The connection fails.

## TERMINAL Class

Each record in the TERMINAL class defines a terminal of the local host, another host on the network, or an X terminal from which a login session can be made. A record also defines terminals that match a terminal name or IP

address *pattern* (using wildcards). Terminal permissions are checked during the user login procedure, so that users cannot succeed in logging in from terminals they have not been authorized to use.

The TERMINAL class also controls administrative access. ADMIN users can only administer Privileged Access Manager from terminals for which they have appropriate access permissions.

When you define a new TERMINAL record, Privileged Access Manager tries to convert the name you provide to a fully qualified name. If it succeeds, it stores the fully qualified name in the database. If it fails, it stores the name you specify. When you issue subsequent commands referencing this record (`chres`, `showres`, `rmres`, `authorize`, and so on), use the name as it appears in the database.

The key of the TERMINAL record is the name of the terminal. This name identifies the terminal to Privileged Access Manager.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessor access types. Each element in the Access Control List (ACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Access**  
Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests
- **success**  
Granted access requests
- **failure**  
Denied access requests (default).
- **none**  
No access requests

Privileged Access Manager records events on each attempted access to a resource. Whether the access rules were applied directly to the resource, group or class that had the resource as a member is not recorded.

Use the audit parameter of the `chres` and `chfile` commands to modify the audit mode.

- **CALACL**

Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the Unicenter NSM calendar status.

Each element in the calendar access control list (CALACL) contains the following information:

- **Accessor**  
Defines an accessor.
- **Calendar**  
Defines a reference to a calendar in Unicenter TNG.
- **Access**  
Defines the access authority that the accessor has to the resource.

Access is permitted only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the `authorize` command to permit user or group access to the resource according to the access defined in the calendar ACL.

- **CALENDAR**



Represents a Unicenter TNG calendar object for user, group, and resource restrictions in Privileged Access Manager. Privileged Access Manager fetches Unicenter TNG active calendars at specified time intervals.

- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource. Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **GROUPS**  
The list of GTERMINAL or CONTAINER records a resource record belongs to.  
To modify this property in a TERMINAL class record, change the MEMBERS property in the appropriate CONTAINER or GTERMINAL record.  
Use the `mem+` or `mem-` parameter with the `chres`, `editres`, or `newres` command to modify this property.
- **NACL**  
The *NACL* property of a resource is an access control list that defines the accessors with authorization denied to a resource, together with the type of access that they are denied (example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Access**  
Defines the type of access that is denied to the accessor.
 Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.
- **NOTIFY**  
Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.  
**Limit:** 30 characters
- **OWNER**  
Defines the user or group that owns the record.
- **PACL**  
Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program Access Control List (PACL) contains the following information:
  - **Accessor**  
Defines an accessor.
  - **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
  - **Access**  
Defines the access authority that the accessor has to the resource.  
**Note:** You can use wildcard characters to specify the resource in a PACL.

Use the `via(pgm)` parameter with the `selang authorize` command to add programs, accessors, and their access types to a PACL. You can use the `authorize-` command to remove accessors from a PACL.

- **SECLABEL**  
Defines the security label of a user or resource.  
**Note:** The SECLABEL property corresponds to the `label[-]` parameter of the `chres` and `ch[x]usr` commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the `ch[x]usr` and `chres` commands.

- **UACC**

Defines the default access authority for the resource. This indicates that the access is granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the `defaccess` parameter with the `chres`, `editres`, or `newres` command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. If Warning mode is enabled on a resource, then all access request to a resource is granted. If an access request violates an access rule, a record is written to the audit log.

**Example 1:** This example shows how to authorize a user to access Selang on a terminal on the local host by using the **TERMINAL** class on a Unix/Linux endpoint.

**Follow these steps:**

1. Create a user "John".

```
PAMSC> eu John password(John_Pwd)
```

2. Log in as "John" user in a different terminal on the same local host, and try to execute Selang commands. John fails to access Selang because by default all users are not authorized to access Selang.

```
ERROR: Initialization failed, EXITING!
(localhost)
ERROR: Login procedure failed
ERROR: You are not allowed to administer this site from terminal MyLocalHost.sample.com
```

3. The superuser (root) creates a policy using **TERMINAL** class that authorizes "John" to access Selang in a terminal on the local host.

```
PAMSC> authorize TERMINAL MyLocalHost.sample.com uid(John) access(r w) (localhost)
```

4. John attempts to access Selang in a terminal on the local host and succeeds.

```
MyLocalHost.sample.com:~> /opt/CA/PAMSC/bin/selang
CA PAMSC selang v12.81.0.2606 - CA PAMSC command line interpreter
Copyright (c) YYYY CA. All rights reserved.
```

**Example 2:** This example shows how to authorize a user to access Selang on a terminal on another host on the network by using the **TERMINAL** class on a Unix/Linux endpoint.

**Follow these steps:**

1. From the local host (MyLocalHost.sample.com), a root user logs in to another host (AnotherHost.sample.com) on the network.

```
MyLocalHost.sample.com:~> ssh root@ AnotherHost.sample.com
root@141.202.41.78's password:

# id
uid=0(root) gid=0(system) groups=2(bin),3(sys),7(security),8(cron),10(audit),11(lp)

# hostname
AnotherHost.sample.com
```

2. The root user accesses Selang, and creates a user "John" in another host on the network (AnotherHost.sample.com).

```
# ./opt/CA/PAMSC/bin/selang
```

```
PAMSC> eu John password(John_pwd)
```

3. From the local host (MyLocalHost.sample.com), John user opens a terminal and logs in to another host (AnotherHost.sample.com) on the network, and attempts to access Selang but fails.

```
MyLocalHost.sample.com:~> ssh John@ AnotherHost.sample.com
```

```
John@141.202.41.78's password:
```

```
$ id
```

```
uid=203(John) gid=1(staff)
```

```
$ hostname
```

```
AnotherHost.sample.com
```

```
$ /opt/CA/PAMSC/bin/selang
```

```
ERROR: Initialization failed, EXITING!
```

```
(localhost)
```

```
ERROR: Login procedure failed
```

```
ERROR: You are not allowed to administer this site from terminal AnotherHost.sample.com
```

4. The root user authorizes John to execute Selang commands in another terminal on the network.

```
PAMSC> authorize terminal AnotherHost.sample.com uid(John) access(r w)
```

5. John can now execute Selang commands in another terminal on the network.

```
$ /opt/CA/PAMSC/bin/selang
```

```
CA PAMSC selang v12.81.0.2690 - CA PAMSC command line interpreter
```

```
Copyright (c) YYYY CA. All rights reserved.
```

## UACC Class

Each record in the UACC class defines the default access allowed to a resource class. The UACC record also determines the access level allowed to a resource of that class that is not protected by Privileged Access Manager.

UACC is applicable to most, but not all, classes. The following table shows how each class uses the UACC class.

UACC Usage	Class
Standard	ADMIN, APPL, AUTHHOST, CALENDAR, CONNECT, CONTAINER, DOMAIN, GAPPL, GAUTHHOST, GHOST, GSUDO, GTERMINAL, HOLIDAY, HOST, HOSTNET, HOSTNP, MFTERMINAL, POLICY, PROCESS, PROGRAM, REGKEY, REGVAL, RULESET, SUDO, SURROGATE, TCP, TERMINAL, USER_DIR, User Defined Classes
Nonstandard	FILE, GFILE
None	AGENT, AGENT_TYPE, CATEGORY, GROUP, PWPOLICY, RESOURCE_DESC, RESPONSE_TAB, SECFILE, SECLABEL, SEOS, SPECIALPGM, USER, USER_ATTR

For users outside the special `_restricted` group, the record for `FILE` in the `UACC` class protects only files that are part of Privileged Access Manager. Examples: the `seos.ini`, `seosd.trace`, `seos.audit`, and `seos.error` files. These files are not explicitly defined to Privileged Access Manager, but are automatically protected by Privileged Access Manager.

The key of the `UACC` class record is the name of the class whose `UACC` properties are being defined.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types.

Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the `access` parameter with the `authorize` or `authorize-` command to modify the ACL.

- **ALLOWACCS**

A list of all allowed accesses for this class.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. `RAUDIT` derives its name from Resource *AUDIT*. Valid values are:

- **all**

All access requests.

- **success**

Granted access requests.

- **failure**

Denied access requests (default).

- **none**

No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the `audit` parameter of the `chres` and `chfile` commands to modify the audit mode.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **NACL**

The `NACL` property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also `ACL`, `CALACL`, `PACL`. Each entry in the `NACL` contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

- **OWNER**

Defines the user or group that owns the record.

- **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## UNIX\_SOCKET Class

Each record in the UNIX\_SOCKET class defines the access that is allowed to a specific Unix Named Socket. You can define a rule even though a Named socket file is not yet created.

### NOTE

: The UNIX\_SOCKET class is not enabled by default.

The key of the UNIX\_SOCKET class record is the name of the socket pathname that is protected by the record. The full path must be specified.

### NOTE

Unix domain sockets with abstract namespaces, instead of pathnames, are also supported on Linux. The key of the UNIX\_SOCKET class, in this case, is the abstract name without the leading null character. For example, the key for unix socket with abstract name "\0hidden" is just "hidden".

The following definitions describe the properties that are contained in this class record. Most properties are modifiable and can be manipulated using Selang or the administration interfaces. Non-modifiable properties are marked informational:

- **ACL** Defines a list of accessors (users and groups) permitted to access the resource, and the accessor access types. Each element in the access control list (ACL) contains the following information:
  - **Accessor** Defines the user or group that is attempting to access the resource under protection.
  - **Access** Defines the access authority that the Accessor has to the resource. Use the Access Parameter with the Authorize or Authorize- command to modify the ACL.
- **CALACL**

Defines a list of the accessors (users and groups) that are permitted to access the resource, and their access types according to the CA Unicenter NSM calendar status. Each element in the Calendar Access Control List (CALACL) contains the following information:

  - **Accessor**

Defines the user or group that is attempting to access the resource under protection.
  - **Calendar**

Defines a reference to a calendar in Unicenter TNG. Use the Calendar parameter with the Authorize command to permit user or group access to the resource according to the access defined in the calendar ACL.
  - **Access**

Defines the access authority that the accessor has to the resource. Access is permitted only when the calendar is ON. Access is denied in all other cases.

- **CALENDAR** Represents a Unicenter TNG calendar object for user, group, and resource restrictions in Privileged Access Manager. Privileged Access Manager fetches Unicenter TNG active calendars at specified time intervals.
- **CATEGORY**  
Defines one or more security categories that are assigned to a user or resource.
- **COMMENT**  
Defines additional information that you can include in the record. Privileged Access Manager does not use this information for authorization. Limit: 255 characters.
- **CREATE\_TIME**  
Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource. Use the Restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property. The resolution of daytime restrictions is one minute.
- **GROUPS**  
The list of GFILE or CONTAINER records a resource record belongs to. DB property: GROUPS  
To modify this property in a FILE class record, change the MEMBERS property in the appropriate CONTAINER or GFILE record. Use the mem+ or mem- parameter with the chres, editres, or newres command to modify this property.
- **NACL**  
The NACL property of a resource is an access control list. The list defines the accessors that are denied authorization to a resource, along with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:
  - **Accessor**  
Defines the user or group that is attempting to access the resource under protection.
  - **Access**  
Defines the type of access that is denied to the accessor. Use the Authorize Deniedaccess command, or the Authorize- Deniedaccess- command, to modify this property.
- **NOTIFY**  
Defines the user to be notified when a resource or user generates an audit event. CA Privileged Identity Manager can email the audit record to the specified user. Limit: 30 characters.
- **Owner**  
Defines the user or group that owns that record.
- **PACL**  
Defines a list of accessors that can access the resource when the access request is made by a specific program, or a program that matches a name pattern and their access types. Each element in the program access control list (PACL) contains the following information:
  - **Accessor**  
Defines the user or group that is attempting to access the resource under protection.
  - **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wild card program matching.
  - **Access**  
Defines the access authority that the accessor has to the resource.  
Use the via(pgm) parameter with the Selang Authorize command to add programs, accessors, and their access types to a PACL. You can use the Authorize- command to remove accessors from a PACL.
- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource AUDIT. Valid values are the following:

- **all**All access requests.
- **success**Granted access requests.
- **failure**Denied access requests.
- **none**No access requests.Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member. Use the audit parameter of the chres and chfile commands to modify the audit mode.
- **SECLABEL**  
Defines the security label of a user or resource.

#### NOTE

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

- **SECLEVEL**Defines the security level of an accessor or resource. This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.
- **UUAC**Defines the default access authority for the resource. This access authority indicates the access tht is granted to accessors who are not defined to Privileged Access Manager or who do not appear inthe ACL of the resource. Use the Defaccess parameter with the chres, editres, or newres command to modify this property.
- **UNTRUST**  
Defines whether the resource is untrusted or trusted. If the UNTRUST property is set, accessors cannot use the resource. If the UNTRUST property is not set, the other properties that are listed in the database for the resource are used to determine accessor access authority. If a trusted resource is changed in any way, Privileged Access Manager sets the UNTRUST property automatically.

Use the trust[-] parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **WARNING**  
Specifies whether Warning mode is enabled. If you enable the Warning mode on a resource, then all the access requests to a resource are granted. If an access request violates an access rule, a record is written to the audit log.

**Example:** This example shows how to restrict user access to allow only user1 to connect to UNIX socket /run/docker.sock and audit all access attempts:

```
AC> so class+(UNIX_SOCKET)
AC> nr UNIX_SOCKET /run/docker.sock owner(nobody) defaccess(none) audit(all)
AC> auth UNIX_SOCKET /run/docker.sock uid(user1) access(connect)
```

## USER Class

Each record in the USER class defines a user in the Privileged Access Manager database.

The key of the USER record is the name of the user entered by the user when logging in to the system.

You can change most of the USER properties from the Privileged Access Manager Endpoint Management, or by using the selang command chusr. Properties that you cannot change using chusr are labeled *informational*.

**NOTE**

Usually, and unless otherwise indicated, to change a property using `chusr`, you use the property name as the command parameter.

You can view all properties from the Privileged Access Manager Endpoint Management or by using the `selang` command `showusr`.

- **APPLIST**  
Used by CA SSO
- **APPLIST\_TIME**  
Used by CA SSO
- **APPLS**  
(Informational) Displays the list of applications that the accessor is authorized to access. Used by CA SSO.
- **AUDIT\_MODE**  
Defines the activities that Privileged Access Manager records in the audit log. You can specify any combination of the following activities:
  - No logging
  - All activities recorded in the trace file
  - Unsuccessful login attempts
  - Successful logins
  - Failed access attempts to resources protected by Privileged Access Manager
  - Successful accesses to resources protected by Privileged Access Manager
  - Interactive logins

**NOTE**

This property corresponds to the audit parameter of the `ch[x]usr` and `ch[x]grp` commands.

- **AUTHNMTHD**  
(Informational) Displays the authentication method or methods to be used with the group record; from method 1 to method 32, or none. Used by CA SSO.
- **BADPASSWD**  
Used by CA SSO
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **COUNTRY**  
A string that specifies a country descriptor for a user. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DAYTIME**  
Defines the day and time restrictions that govern when an accessor can access a resource.  
Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.  
The resolution of daytime restrictions is one minute.
- **EMAIL**  
Defines the email address of the user, up to 128 characters.
- **EXPIRE\_DATE**  
Defines the date on which an accessor becomes invalid. A value for the `EXPIRE_DATE` property in a user record overrides a value in a group record.



**Note:** This property corresponds to the expire[-] parameter of the ch[x]usr and ch[x]grp commands.

- **FULLNAME**

Defines the full name associated with an accessor. Privileged Access Manager uses the full name to identify the accessor in audit log messages, but not for authorization.

**NOTE**

FULLNAME is an alphanumeric string. The maximum length for groups and users is 255 characters.

- **GAPPLS**

(Informational) Indicates the list of application groups that the user is authorized to access. Used by CA SSO.

- **GRACELOGIN**

Defines the number of grace logins a user has after a password expires. When the number of grace logins is exceeded, the user is denied access to the system and must contact the system administrator for a new password.

The number of grace logins must be from 0 through 255. If this value is 0, the user cannot log in.

A value for the GRACELOGIN property in a USER record overrides a value for NGRACE in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

**NOTE**

This property corresponds to the grace parameter of the ch[x]usr command.

- **GROUPS**

(Informational) Displays the list of user groups that the user belongs to. This property also contains any group authorities, such as group administration authority (GROUP-ADMIN), assigned to the user for each group the user belongs to.

The group list that is contained in this property can be different from the one in the native environment GROUPS property.

**Note:** The ch[x]usr command does not modify this property. Instead, use the join[-] or joinx[-] command to modify this property.

- **HOMEDIR**

(UNIX only) Defines the home directory of the user. Used by CA SSO.

- **INACTIVE**

Defines the number of days of inactivity that must pass before the system changes the status of a user to inactive. If the account status is inactive, the user cannot log in.

A value for the INACTIVE property in a USER record overrides a value in a GROUP record. Both override the INACT property in the SEOS class record.

**NOTE**

Privileged Access Manager does not store the status; it calculates the status dynamically. To identify inactive users, you must compare the INACTIVE value with the LAST\_ACC\_TIME value of the user.

- **LAST\_ACC\_TERM**

Displays the terminal from which the last login was performed.

- **LAST\_ACC\_TIME**

Displays the date and time of the last login.

- **LOCALAPPS**

Used by CA SSO

- **LOCATION**

Defines a user location. Privileged Access Manager does not use this information for authorization.

- **LOGININFO**

Defines the information to log the user in to a specific application and audit data. LOGININFO contains a separate list for each application that the user is authorized to access. Used by CA SSO.

- **LOGSHIFT**

Indicates whether a login outside of the shift time frame is permitted. Privileged Access Manager writes an audit record in the audit log for this event.

- **MAXLOGINS**

Defines the maximum number of concurrent logins that a user is allowed. A zero value indicates that the user can have any number of concurrent logins.

A value for the MAXLOGINS property in a user record overrides a value in a group record. Both override the value of MAXLOGINS in the SEOS class record.

- **MIN\_TIME**

Defines the minimum time in days allowed between password changes for the user.

A value for the MIN\_TIME property in a USER record overrides a value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

**Note:** This property corresponds to the min\_life parameter of the ch[x]usr command.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters

- **OBJ\_TYPE**

Specifies the user authority attributes. Each of these attributes corresponds to the parameter of the same name in the ch[x]usr command. A user can have one or more of the following authority attributes:

- **ADMIN**

Specifies whether the user can perform administrative functions, similar to root in the UNIX environment.

- **AUDITOR**

Specifies whether the user can monitor the system, list information in the database, and can set the audit mode for existing records.

- **IGN\_HOL**

Specifies whether the user can log in during any timeframe defined in a HOLIDAY record.

- **LOGICAL**

Specifies that the user is only for internal Privileged Access Manager purposes and cannot be used by a real user to log in.

For example, the user nobody that you can use as the owner of resources to prevent even the resource owner from accessing the resource is a logical user by default. This means that no user can log in using this account.

- **OPERATOR**

Specifies whether the user can list everything in the database and can use the secons utility.

- **PWMANAGER**

Specifies whether the user can modify the password settings of other users and can enable a user account that the serevu utility has disabled.

- **SERVER**

Specifies whether a process can ask users for authorization and can issue the SEOSROUTE\_VerifyCreate API call.

- **OIDCRDDATA**

Used by CA SSO

- **OLD\_PASSWD**

Contains an encrypted list of the previous passwords of the user. The user cannot choose a new password from this list. The maximum number of passwords that are saved in OLD\_PASSWD is determined by the setoptions command.

- **ORG\_UNIT**

A string that stores information about the organizational unit in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.

- **ORGANIZATION**

Defines the organization in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use this string for authorization.

- **OWNER**

Defines the user or group that owns the record.

- **PASSWD\_A\_C\_W**

Indicates the ADMIN user who last changed the user password for this record.

- **PASSWD\_INT**

Defines the maximum time in days between password changes for users.

A value for the PASSWD\_INT property in a USER record overrides the value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

#### NOTE

This property corresponds to the interval parameter of the ch[x]usr command.

- **PASSWD\_L\_A\_C**

Displays the date and time at which an administrator last updated the password.

- **PASSWD\_L\_C**

Displays the date and time at which a user last updated the password.

- **PGMINFO**

Defines the program information that Privileged Access Manager generates automatically.

The Watchdog automatically verifies the information stored in this property. If it is changed, Privileged Access Manager defines the program as untrusted.

You can select any of the following flags to *exclude* the associated information from this verification process:

- **crc**

The cyclic redundancy check and MD5 signature.

- **ctime**

(UNIX only) The time of the last file status change.

- **device**

On UNIX, the logical disk that the file resides on. On Windows, the drive number of the disk containing the file.

- **group**

The group that owns the program file.

- **inode**

On UNIX, the file system address of the program file. On Windows, this flag has no meaning

- **mode**

The associated security protection mode for the program file.

- **mtime**

The time the program file was last modified.

- **owner**

The user who owns the program file.

- **sha1**

The SHA1 signature. Digital signature method that is named Secure Hash Algorithm that could be applied to the program or sensitive files.

- **size**

The size of the program file.

Use the flags, flags+, or flags- parameter with the chres, editres, or newres command to modify the flags in this property.

- **PHONE**

Defines the user's telephone number. This information is not used for authorization.

- **POLICYMODEL**

Specifies the PMDB that receives new passwords when you change user passwords with the sepass utility. The passwords are *not* sent to the Policy Model defined by the parent\_pmd or passwd\_pmd configuration settings if a value is entered for this property.

**Note:** This property corresponds to the pmdb[-] parameter of the ch[x]usr and ch[x]grp commands.

- **PROFILE**

Defines the path to the profile of a user. This string can include a local absolute path, or a UNC path.

- **PWD\_AUTOGEN**

Displays whether the user password is automatically generated. Used by CA SSO.

The default is no.

- **PWD\_SYNC**

Displays whether the user password is automatically kept identical for all user applications. Used by CA SSO.  
The default is no.

- **RESUME\_DATE**

Defines the date on which a suspended USER account becomes unsuspended.  
RESUME\_DATE and SUSPEND\_DATE work together.

**NOTE**

This property corresponds to the resume[-] parameter of the ch[x]usr and ch[x]grp commands.

- **REVACL**

Displays the access control lists of the accessor.

- **REVOKE\_COUNT**

Used by CA SSO

- **SCRIPT\_VARS**

Used by CA SSO, Defines a variables list with the variable values of the application script that are saved per application.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

- **SESSION\_GROUP**

Defines an SSO session group for a user. The SESSION\_GROUP property is a string with a maximum length of 16 characters.

In Windows, an administrator can enter a session group new name if the preferred name is not in the drop-down list.

Used by CA SSO

- **SHIFT**

Used by CA SSO

- **SUSPEND\_DATE**

Defines the date on which a user account is suspended and so becomes invalid.

If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.

If a user has a resume date that is earlier than the suspend date, the record is also invalid *before* the resume date. The user can work only between the resume and suspend dates.

A value for the SUSPEND\_DATE property in a user record overrides the value in a group record.

**NOTE**

This property corresponds to the suspend[-] parameter of the ch[x]usr and ch[x]grp commands.

- **SUSPEND\_WHO**

Displays the administrator who activated the suspend date.

**Note:** This property corresponds to the suspend[-] parameter of the ch[x]usr command.

- **UALIAS**

Displays the aliases of a specific user-defined to one or more authentication hosts. Used by CA SSO.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

## USER\_ATTR Class

Each record in the USER\_ATTR class defines the valid user attributes of a CA SSO user directory.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ATTR\_PREDEFS**  
The list of allowed values for a specific attribute.
- **ATTRNAME**  
(Informational). The name of the attribute.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DBFIELD**  
The name of the field in the userdir database. Since different databases can contain different attributes, the attribute fields should be synchronized.
- **FIELDID**  
(Informational). The ID of the DB field
- **OWNER**  
Defines the user or group that owns the record.
- **PARAMETER\_TYPE**  
Indicates whether the user attribute is a string or numeric.
- **PRIORITY**  
The priority of the user attribute: when setting an authorization rule to a PARAM\_RULE object (such as APPL, URL) the rule is defined with the priority that the user attribute refers to.
- **RAUDIT**  
Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:
  - **all**  
All access requests.
  - **success**  
Granted access requests.
  - **failure**  
Denied access requests (default).
  - **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.
- **USER\_DIR\_PROP**  
(Informational). The name of the user's directory.
- **USERATTR\_FLAGS**

Contains information about the attribute. The flag can contain the following values:

- **aznchk**-Indicates whether to use this attribute for authorization.
- **predef** (predefined), **freetex** (free text), or **userdir** (user directory)-These three values specify the source of the user attributes.
- **user** or **group**-These values indicate whether the attribute (accessor) is a user or a group.
- **WARNING**  
Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## USER\_DIR Class

Each record in the USER\_DIR class defines a CA SSO user directory.

The key of the USER\_DIR record is the name of the directory.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ADMIN\_NAME**  
Login name of the administrator of the directory.
- **ADMIN\_PWD**  
Password of the administrator of the directory. The password is stored in clear text format. It is not displayed in selang but can be obtained with seadmap functions.
- **AZNACL**  
Defines the authorization ACL. The authorization ACL is an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. Typically, when an AZNACL is used, the object is not in the database.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **CONTOBJ\_CLS**  
The names of the classes the container object inherits from (needed for creation of new login info containers in LDAP.)
- **CREATE\_TIME**  
(Informational) Displays the date and time when the record was created.
- **DIR\_TYPE**  
The type of directory. Valid values are: ETRUST\_AC, LDAP, ODBC, NT\_Domain or none.
- **GRPOBJ\_CLS**  
The names of the classes the group object inherits from (needed for creation of new groups in LDAP.)
- **LICONTOBJ\_CLS**  
The names of the classes the login info container object inherits from (needed for creation of new login info containers in LDAP.)
- **LIOBJ\_CLS**  
The names of the classes the login info object inherits from (needed for creation of new login information in LDAP.)
- **MAX\_RET\_ITEMS**  
The maximum number of items retrieved. The default depends on the directory type.
- **OWNER**  
Defines the user or group that owns the record.
- **PATH**  
The relative distinguishing name in the LDAP tree to begin all queries.
- **PORT\_NUM**

The port number on the host computer used to access the directory.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the audit parameter of the chres and chfile commands to modify the audit mode.

- **TIMEOUT\_CON**

The time (in seconds) the system waits to connect to the directory before issuing a Timeout error message.

- **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **USERATTR\_LIST**

The list of objects in the USER\_ATTR class that was created with this USER\_DIR object as the value for the USER\_DIR parameter.

- **USERDIR\_HOST**

The name of the host computer for the directory. This property must be defined in the class record.

- **USROBJ\_CLS**

The names of the classes the user object inherits from (needed for creation of new users in LDAP.)

- **VERSION**

The version number of the directory.

## WEBSERVICE Class

The WEBSERVICE class is obsolete; it is not used by Privileged Access Manager.

## WINSERVICE Class

Each record in the WINSERVICE class defines a Windows Service. Use records in the WINSERVICE class to define access rules for Windows Services.

The key of a WINSERVICE class record is the Windows name of the service.

**Note:** In most cases, and unless otherwise indicated, to change a property using the selang chres command, you use the property name as the command parameter.

You can view all properties from the Privileged Access Manager Endpoint Management or by using the `selang` command `showres WINSERVICE`.

- **ACL**

Defines a list of accessors (users and groups) permitted to access the resource, and the accessors' access types. Each element in the access control list (ACL) contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the access authority that the accessor has to the resource.

Use the access parameter with the `authorize` or `authorize-` command to modify the ACL.

- **CATEGORY**

Defines one or more security categories assigned to a user or a resource.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **GROUPS**

Defines the list of CONTAINER records that a resource record belongs to.

To modify this property in a class record, change the MEMBERS property in the appropriate CONTAINER record.

Use the `mem+` or `mem-` parameter with the `chres`, `editres` or `newres` command to modify this property.

- **NACL**

The *NACL* property of a resource is an access control list that defines the accessors that are denied authorization to a resource, together with the type of access that they are denied (for example, write). See also ACL, CALACL, PACL. Each entry in the NACL contains the following information:

- **Accessor**

Defines an accessor.

- **Access**

Defines the type of access that is denied to the accessor.

Use the `authorize deniedaccess` command, or the `authorize- deniedaccess-` command, to modify this property.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

- **OWNER**

Defines the user or group that owns the record.

- **PACL**

Defines a list of accessors that are permitted to access the resource when the access request is made by a specific program (or a program that matches a name-pattern) and their access types. Each element in the program access control list (PACL) contains the following information:



- – **Accessor**  
Defines an accessor.
- **Program**  
Defines a reference to a record in the PROGRAM class, either specifically or by wildcard pattern matching.
- **Access**  
Defines the access authority that the accessor has to the resource.

**NOTE**

You can use wildcard characters to specify the resource in a PACL.

Use the *via(pgm)* parameter with the *selang authorize* command to add programs, accessors, and their access types to a PACL. You can use the *authorize-* command to remove accessors from a PACL.

- **RAUDIT**

Defines the types of access events that Privileged Access Manager records in the audit log. RAUDIT derives its name from Resource *AUDIT*. Valid values are:

- – **all**  
All access requests.
- **success**  
Granted access requests.
- **failure**  
Denied access requests (default).
- **none**  
No access requests.

Privileged Access Manager records events on each attempted access to a resource, and does not record whether the access rules were applied directly to the resource, or were applied to a group or class that had the resource as a member.

Use the *audit* parameter of the *chres* and *chfile* commands to modify the audit mode.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the *label[-]* parameter of the *chres* and *ch[x]usr* commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the *level[-]* parameter of the *ch[x]usr* and *chres* commands.

- **UACC**

Defines the default access authority for the resource, which indicates the access granted to accessors who are not defined to Privileged Access Manager or who do not appear in the ACL of the resource.

Use the *defaccess* parameter with the *chres*, *editres*, or *newres* command to modify this property.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **WARNING**

Specifies whether Warning mode is enabled. When Warning mode is enabled on a resource, all access requests to the resource are granted, and if an access request violates an access rule, a record is written to the audit log.

## XGROUP Class

Each record in the XGROUP class defines a group of users in the database.

The key of each XGROUP class record is the name of the group.

### NOTE

The properties of profile groups apply to each user associated with the profile group. However, if the same property is specified in a user (USER or XUSER) record, the user record overrides those in the profile group record.

You can change most of these properties from the Privileged Access Manager Endpoint Management, or by using the `selang` command `chxgrp`.

### NOTE

Usually, and unless otherwise indicated, to change a property using `chxgrp`, you use the property name as the command parameter.

You can view all properties from the Privileged Access Manager Endpoint Management, or by using the `selang` command `showxgrp`.

- **APPLS**

(Informational) Displays the list of applications that the accessor is authorized to access. Used by CA SSO.

- **AUDIT\_MODE**

Defines the activities that Privileged Access Manager records in the audit log. You can specify any combination of the following activities:

- No logging
- All activities recorded in the trace file
- Unsuccessful login attempts
- Successful logins
- Failed access attempts to resources protected by Privileged Access Manager
- Successful accesses to resources protected by Privileged Access Manager
- Interactive logins

### NOTE

This property corresponds to the audit parameter of the `ch[x]usr` and `ch[x]grp` commands. You can use `AUDIT_MODE` for a GROUP or XGROUP to set the audit mode for all members of the group. However, you cannot use `AUDIT_MODE` to set the audit mode for group members if a user's audit mode is defined in a USER record, XUSER record, or profile group.

- **AUTHNMTHD**

(Informational) Displays the authentication method or methods to be used with the group record; from method 1 to method 32, or none. Used by CA SSO.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the `chres`, `ch[x]usr`, or `ch[x]grp` commands to modify this property.

The resolution of daytime restrictions is one minute.

- **EXPIRE\_DATE**  
Defines the date on which an accessor becomes invalid. A value for the EXPIRE\_DATE property in a user record overrides a value in a group record.  
**Note:** This property corresponds to the expire[-] parameter of the ch[x]usr and ch[x]grp commands.
- **FULLNAME**  
Defines the full name associated with an accessor. Privileged Access Manager uses the full name to identify the accessor in audit log messages, but not for authorization.  
FULLNAME is an alphanumeric string. For groups, the maximum length is 255 characters. For users, the maximum length is 47 characters.
- **GAPPLS**  
Defines the list of application groups that the group is authorized to access. Used by CA SSO.
- **GROUP\_MEMBER**  
Defines the groups that are members of this group.
- **GROUP\_TYPE**  
Specifies the group authority attributes. Each of these attributes corresponds to the parameter of the same name in the ch[x]grp command. A group can have one or more of the following authority attributes:
  - **ADMIN**  
Specifies whether a user who belongs to the group can perform administrative functions, similar to root in the UNIX environment.
  - **AUDITOR**  
Specifies whether a user who belongs to the group can monitor the system, list information in the database, and can set the audit mode for existing records.
  - **OPERATOR**  
Specifies whether a user who belongs to the group can list everything in the database and can use the secons utility.
  - **PWMANAGER**  
Specifies whether a user who belongs to the group can modify the password settings of other users and can enable a user account that the serevu utility has disabled.
  - **SERVER**  
Specifies whether a process can ask users who belong to the group for authorization and can issue the SEOSROUTE\_VerifyCreate API call.
- **MEMBER\_OF**  
Defines the groups that this group is a member of.
- **OWNER**  
Defines the user or group that owns the record.
- **PROFUSR**  
Displays a list of the users associated with this profile group.
- **PWD\_AUTOGEN**  
Indicates whether the group password is automatically generated. The default is no. Used by CA SSO.
- **PWD\_SYNC**  
Indicates whether the group password is automatically kept identical for all group applications. The default is no. Used by CA SSO.
- **PWPOLICY**  
Defines the record name of the password policy for the group. A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. The default is no validity check. Used by CA SSO.
- **REVACL**  
Displays the access control lists of the accessor.
- **SHELL**  
(UNIX only) The shell program that is assigned to a new UNIX user when the user is a member of this group.

Use the shellprog parameter with the chxgrp command to modify this property.

- **SUBGROUP**

Displays the list of groups that have this group as a parent.

- **SUPGROUP**

Defines the name of the parent group (superior group).

Use the parent[-] parameter with the ch[x]grp command to modify this property.

- 

- **SUSPEND\_DATE**

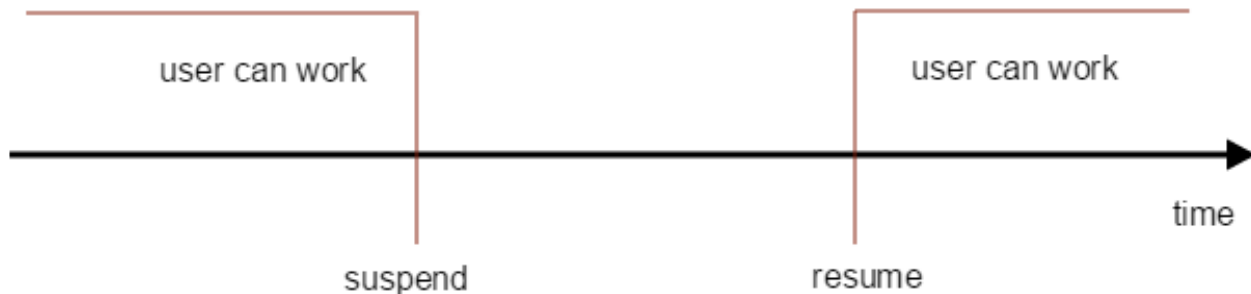
Defines the date on which a user account is suspended and so becomes invalid.

If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.

**NOTE**

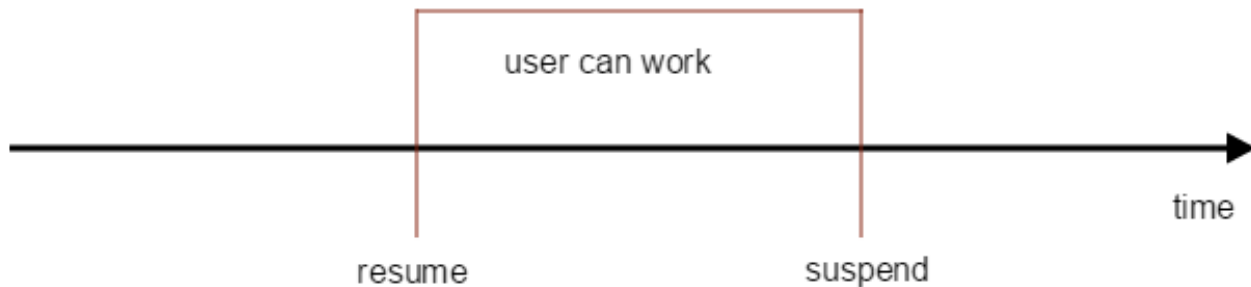
This property corresponds to the suspend[-] parameter of the ch[x]usr and ch[x]grp commands.

**Figure 55: XGROUP Class 1**



If a user has a resume date that is earlier than the suspend date, the record is also invalid *before* the resume date. The user can work only between the resume and suspend dates.

**Figure 56: XGROUP\_Class\_2**



- A value for the SUSPEND\_DATE property in a user record overrides the value in a group record.

- **SUSPEND\_WHO**

Displays the administrator who activated the suspend date.

- **UPDATE\_TIME**

(Informational) Displays the date and time when the record was last modified.

- **UPDATE\_WHO**

(Informational) Displays the administrator who performed the update.

- **USERLIST**

Displays the users that belong to the group.

The user list that is contained in this property may be different from the one in the native environment USERS property.

## XUSER Class

Each record in the XUSER class defines an enterprise user in the database.

The key of the XUSER record is the name of the user entered by the user when logging in to the system.

You can change most of these properties from the Privileged Access Manager Endpoint Management or by using the `selang` command `chxusr`.

### NOTE

Usually, and unless otherwise indicated, to change a property using `chxusr`, you use the property name as the command parameter.

You can view all properties from Privileged Access Manager Endpoint Management or by using the `selang` command `showxusr`.

- **APPLIST**  
Used by CA SSO.
- **APPLIST\_TIME**  
Used by CA SSO.
- **APPLS**  
(Informational) Displays the list of applications that the accessor is authorized to access. Used by CA SSO.
- **AUDIT\_MODE**  
Defines the activities that Privileged Access Manager records in the audit log. You can specify any combination of the following activities:
  - No logging
  - All activities recorded in the trace file
  - Unsuccessful login attempts
  - Successful logins
  - Failed access attempts to resources protected by Privileged Access Manager
  - Successful accesses to resources protected by Privileged Access Manager
  - Interactive logins

### NOTE

This property corresponds to the audit parameter of the `ch[x]usr` and `ch[x]grp` commands.

- **AUTHNMTD**  
(Informational) Displays the authentication method or methods to be used with the group record; from method 1 to method 32, or none. Used by CA SSO.
- **BADPASSWD**  
Used by CA SSO.
- **CATEGORY**  
Defines one or more security categories assigned to a user or a resource.
- **COMMENT**  
Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
**Limit:** 255 characters.
- **COUNTRY**  
A string that specifies a country descriptor for a user. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.
- **CREATE\_TIME**

(Informational) Displays the date and time when the record was created.

- **DAYTIME**

Defines the day and time restrictions that govern when an accessor can access a resource.

Use the restrictions parameter with the chres, ch[x]usr, or ch[x]grp commands to modify this property.

The resolution of daytime restrictions is one minute.

- **EMAIL**

Defines the email address of the user, up to 128 characters.

- **FULLNAME**

Defines the full name associated with an accessor. Privileged Access Manager uses the full name to identify the accessor in audit log messages, but not for authorization.

FULLNAME is an alphanumeric string. For groups the maximum length is 255 characters. For users, the maximum length is 47 characters.

- **GAPPLS**

(Informational) Indicates the list of application groups that the user is authorized to access. Used by CA SSO.

- **GRACELOGIN**

Defines the number of grace logins a user has after a password expires. When the number of grace logins is exceeded, the user is denied access to the system and must contact the system administrator for a new password.

The number of grace logins must be from 0 through 255. If this value is 0, the user cannot log in.

A value for the GRACELOGIN property in a USER record overrides a value for NGRACE in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

**NOTE**

This property corresponds to the grace parameter of the ch[x]usr command.

- **GROUPS**

(Informational) Displays the list of user groups that the user belongs to. This property also contains any group authorities, such as group administration authority (GROUP-ADMIN), assigned to the user for each group the user belongs to.

The group list that is contained in this property can be different from the one in the native environment GROUPS property.

**Note:** This property is not modified by the ch[x]usr command. Instead, use the join[-] or joinx[-] command to modify this property.

- **INACTIVE**

Defines the number of days of inactivity that must pass before the system changes the status of a user to inactive. If the account status is inactive, the user cannot log in.

A value for the INACTIVE property in a USER record overrides a value in a GROUP record. Both override the INACT property in the SEOS class record.

**NOTE**

Privileged Access Manager does not store the status; it calculates the status dynamically. To identify inactive users, you must compare the INACTIVE value with the LAST\_ACC\_TIME value of the user.

- **LAST\_ACC\_TERM**

Displays the terminal from which the last login was performed.

- **LAST\_ACC\_TIME**

Displays the date and time of the last login.

- **LOCALAPPS**

Used by CA SSO.

- **LOCATION**

Defines a user location. Privileged Access Manager does not use this information for authorization.

- **LOGININFO**

Defines the information to log the user in to a specific application and audit data. LOGININFO contains a separate list for each application that the user is authorized to access. Used by CA SSO.

- **LOGSHIFT**

Indicates whether a login outside of the shift time frame is permitted. Privileged Access Manager writes an audit record in the audit log for this event.

- **MAXLOGINS**

Defines the maximum number of concurrent logins that a user is allowed. A zero value indicates that the user can have any number of concurrent logins.

A value for the MAXLOGINS property in a user record overrides a value in a group record. Both override the value of MAXLOGINS in the SEOS class record.

- **MIN\_TIME**

Defines the minimum time in days allowed between password changes for the user.

A value for the MIN\_TIME property in a USER record overrides a value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

**Note:** This property corresponds to the min\_life parameter of the ch[x]usr command.

- **NOTIFY**

Defines the user to be notified when a resource or user generates an audit event. Privileged Access Manager can email the audit record to the specified user.

**Limit:** 30 characters.

- **OBJ\_TYPE**

Specifies the user authority attributes. Each of these attributes corresponds to the parameter of the same name in the ch[x]usr command. A user can have one or more of the following authority attributes:

- **ADMIN**

Specifies whether the user can perform administrative functions, similar to root in the UNIX environment.

- **AUDITOR**

Specifies whether the user can monitor the system, list information in the database, and can set the audit mode for existing records.

- **IGN\_HOL**

Specifies whether the user can log in during any period of time defined in a HOLIDAY record.

- **LOGICAL**

Specifies that the user is only for internal Privileged Access Manager purposes, and cannot be used by a real user to log in.

For example, the user nobody that you can use as the owner of resources to prevent even the resource owner from accessing the resource is a logical user by default. This means that no user can log in using this account.

- **OPERATOR**

Specifies whether the user can list everything in the database and can use the secons utility.

- **PWMANAGER**

Specifies whether the user can modify the password settings of other users and can enable a user account that the serevu utility has disabled.

- **SERVER**

Specifies whether a process can ask users for authorization and can issue the SEOSROUTE\_VerifyCreate API call.

- **OIDCRDDATA**

Used by CA SSO.

- **OLD\_PASSWD**

Contains an encrypted list of the previous passwords of the user. The user cannot choose a new password from this list. The maximum number of passwords that are saved in OLD\_PASSWD is determined by the setoptions command.

- **ORG\_UNIT**

A string that stores information about the organizational unit in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.

- **ORGANIZATION**

Defines the organization in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use this for authorization.

- **PASSWD\_A\_C\_W**

Indicates the ADMIN user who last changed the user password for this record.

- **PASSWD\_INT**

Defines the maximum time in days between password changes for users.

A value for the PASSWD\_INT property in a USER record overrides the value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

**NOTE**

This property corresponds to the interval parameter of the ch[x]usr command.

- **PASSWD\_L\_A\_C**

Displays the date and time at which an administrator last updated the password.

- **PASSWD\_L\_C**

Displays the date and time at which a user last updated the password.

- **PHONE**

Defines the telephone number of the user. This information is not used for authorization.

- **PWD\_AUTOGEN**

Displays whether the user password is automatically generated. Used by CA SSO.

The default is no.

- **PWD\_SYNC**

Displays whether the user password is automatically kept identical for all user applications. Used by CA SSO.

The default is no.

- **REVACL**

Displays the access control lists of the accessor.

- **REVOKE\_COUNT**

Used by CA SSO.

- **SCRIPT\_VARS**

Used by CA SSO, Defines a variables list with the variable values of the application script that are saved per application.

- **SECLABEL**

Defines the security label of a user or resource.

**NOTE**

The SECLABEL property corresponds to the label[-] parameter of the chres and ch[x]usr commands.

- **SECLEVEL**

Defines the security level of an accessor or resource.

**Note:** This property corresponds to the level[-] parameter of the ch[x]usr and chres commands.

- **SESSION\_GROUP**

Defines an SSO session group for a user. The SESSION\_GROUP property is a string with a maximum length of 16 characters.

In Windows, an administrator can enter a session group new name if the preferred name is not in the drop-down list.

Used by CA SSO.

- **SHIFT**

Used by CA SSO.

- **SUSPEND\_DATE**

Defines the date on which a user account is suspended and so becomes invalid.

If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.

If a user has a resume date that is earlier than the suspend date, the record is also invalid *before* the resume date. The user can work only between the resume and suspend dates.

A value for the SUSPEND\_DATE property in a user record overrides the value in a group record.



**NOTE**

This property corresponds to the `suspend[-]` parameter of the `ch[x]usr` and `ch[x]grp` commands.

- **SUSPEND\_WHO**  
Displays the administrator who activated the suspend date.
- **UALIAS**  
Displays the aliases of a specific user defined to one or more authentication hosts. Used by CA SSO.
- **UPDATE\_TIME**  
(Informational) Displays the date and time when the record was last modified.
- **UPDATE\_WHO**  
(Informational) Displays the administrator who performed the update.

## Classes in the Windows Environment

The topics in this section describe the Windows classes and properties in the Windows database (classes in the *nt environment*).

**NOTE**

The term *nt environment* refers to the database accessed with the `selang env nt` command. This is the same database the Windows operating system maintains for users, groups, and resources.

Use the table of contents to the left to access the topics.

### COM Class

Each record in the COM class defines a device specifying a serial port (COM) or a parallel port (LPT) as listed in the Windows Control Panel, Ports.

**NOTE**

You cannot create new objects in the COM class using Privileged Access Manager.

The key of the COM class is the name of the port being controlled.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **DEV**  
(Informational). A string to indicate the device serial number.
- **DACL**  
Defines the standard access control list that contains the user names and group names authorized to access the resource, and the level of access granted to each.  
Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).  
Each element in the access control list contains the following information:
  - **Access Type**  
Specifies permissions to the resource:
    - a. **Allowed**-Permits special access to the resource.
    - b. **Denied**-Denies special access to the resource.
  - **Accessor**  
The user or group for whom the access rights are allowed or denied.
  - **Access**  
The access authority that the accessor has to the resource.

**NOTE**

In an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use `auth` or `auth-` command to modify this property.

- **GID**  
Displays the group information for the file or device.
- **OWNER**  
Defines the user or group that owns the record.
- **SACL**  
Windows System Access Control List. Displays audit directives.

**DEVICE Class**

Each record in the DEVICE class defines a Windows hardware device as listed in the Windows Control Panel, Devices.

The key of the DEVICE class record is the name of the device being controlled.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **STARTUPTYPE**  
Defines how (when) the device is started. Options are:
  - **automatic**  
Starts the device automatically during system startup.
  - **boot**  
Starts the device every time the system starts, before any other devices start. Select this option for critical devices essential to system operation.
  - **disabled**  
Prevents users from starting the device. The system can still start disabled devices.
  - **manual**  
Allows the device to be started by a user or a dependent device.
  - **system**  
Starts the device every time the system starts, after the Boot devices start. Select this option for critical devices essential to system operation.

Use the `starttype` parameter with the `chres` or `editres` commands to modify this property.
- **STATUS**  
Changes the current service state. Options are: `started`, `stopped`, and `paused`.  
Use the `status` parameter with the `chres` or `editres` commands to modify this property.
- **IMAGEPATH**  
The fully qualified path for the specified device.
- **PROFILE**  
A string that specifies a path to the user's profile. This string can include a local absolute path, or a UNC path.  
Use the `profile` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

**Example: Activate a modem**

To display the status of the modem, enter the `selang` command:

```
showres DEVICE modem
```

To activate the modem, enter the command:

```
chres device modem status(started)
```

## DISK Class

Each record in the DISK class defines a system volume. Volume is the general term that refers to any of the entities that you can create and use on a computer running Windows operating systems (Server editions) such as a primary partition, a logical drive in an extended partition, a volume set, a stripe set, a mirror set, or a stripe set with parity. A volume has a single drive letter assigned to it and is formatted for use by a file system.

### NOTE

You cannot create objects in the DISK class using Privileged Access Manager.

The key of the DISK class is the assigned drive letter (C:, D:, and so on).

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using *selang* or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ATIME**  
(Informational). The time the record was last accessed.
- **CTIME**  
(Informational). Created time.
- **DACL**  
Defines the standard access control list that contains the user names and group names authorized to access the resource, and the level of access granted to each.  
Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).  
Each element in the access control list contains the following information:
  - **Access Type**  
Specifies permissions to the resource:
    - a. **Allowed**-Permits special access to the resource.
    - b. **Denied**-Denies special access to the resource.
  - **Accessor**  
The user or group for whom the access rights are allowed or denied.
  - **Access**  
The access authority that the accessor has to the resource.

### NOTE

In an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use *auth* or *auth-* command to modify this property.

- **FILE\_SYSTEM**  
(Informational). A name to designate the file system (such as FAT or NTFS).
- **FREE\_SPACE**  
(Informational). The total amount of free space (in KB) on the disk.
- **GID**  
Displays the group information for the file or device.
- **LABEL**  
(Informational). The name of the specified volume.
- **LINK\_NUMB**  
(Informational). Specifies the number of links. For non-NTFS file systems, this property is always one.
- **MTIME**  
(Informational). The time the record was last modified.
- **OWNER**  
Defines the user or group that owns the record.
- **SACL**

Windows System Access Control List. Displays audit directives.

- **TYPE**  
(Informational). Specifies whether the disk is removable, fixed, a CD-ROM, a RAM disk, or a network drive.
- **USED\_SPACE**  
(Informational). The total amount of used space (in KB) on the disk.

## DOMAIN Class (Windows Environment)

Each record in the DOMAIN class defines a collection of computers that share a common database and security policy (domain). A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.

### NOTE

You cannot create new objects in the DOMAIN class using Privileged Access Manager.

The key to the DOMAIN record is the domain name.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **BDC**  
(Informational). The name of the computer that receives a copy of the domain's directory database and contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). Backup domain controllers (BDCs) also authenticate user logins and can be promoted to function as PDCs as needed. Multiple BDCs can exist on a domain.
- **COMPUTERS**  
Lists computers that are the members of the specified domain.  
Use `computer` or `computer-` parameter with the `chres` and `editres` commands to modify this property.
- **DOMAIN\_NAME**  
Defines the domain name.
- **DOMAIN\_USERS**  
(Informational). Lists user and group accounts that are members of the specified domain.
- **PDC**  
(Informational). The name of the first computer created in the domain; this computer contains the primary storehouse for domain data. It authenticates domain logins and maintains the directory database for a domain. The primary domain controller (PDC) tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC.
- **TRUSTED**  
Lists trusted and trusting domains.  
A trust relationship is a link between domains that allows pass-through authentication, in which a trusting domain honors the login authentications of a trusted domain. With trust relationships, a user with only one user account in one domain can potentially access the entire network. You can give user accounts and global groups defined in a trusted domain rights and resource permissions in a trusting domain, even though those accounts do not exist in the trusting domain's directory database.  
Use the `trusted` or `trusting-` parameter with the `chres` and `editres` commands to modify this property. You should specify a password for this command.
- **TRUSTING**  
The Trusting domain are domains which trust the target domain.

## FILE Class (Windows Environment)

Valid in the Windows environment

Each record in the FILE class defines a file on a file system (for example, FAT, NTFS, or CDFS) on a physical or logical drive of a computer.

**NOTE**

You cannot use Privileged Access Manager to physically create files on disk.

The key of the FILE class record is the name of the file or directory protected by the record. The full path must be specified.

The following definitions describe the properties contained in a FILE record. You can use `selang` or the Web based GUI to change the record's modifiable properties.

- **ATIME**  
Displays the time the file was last accessed.
- **ATTRIB**  
Displays attributes for the file or directory. The attributes can be one or more of the following:
  - ARCHIVE
  - COMPRESSED
  - DIRECTORY
  - HIDDEN
  - NORMAL
  - OFFLINE
  - READONLY
  - SYSTEM
  - TEMPORARY
- **CTIME**  
Displays the created time.
- **DACL**  
Defines the standard access control list that contains the user names and group names authorized to access the resource, and the level of access granted to each.  
Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).  
Each element in the access control list contains the following information:
  - **Access Type**  
Specifies permissions to the resource:
    - a. **Allowed**-Permits special access to the resource.
    - b. **Denied**-Denies special access to the resource.
  - **Accessor**  
The user or group for whom the access rights are allowed or denied.
  - **Access**  
The access authority that the accessor has to the resource.

**NOTE**

In an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use `auth` or `auth-` command to modify this property.

- **DEV**  
Displays the serial number of the volume where the file is located.
- **FILE\_SYSTEM**  
Displays the name of the file system where the file is located.
- **GID**

Displays the group information for the file or device.

- **INDEX**  
Displays the unique identifier associated with the file.
- **ISDIR**  
Indicates whether the file is a directory.
- **LINKS\_NUMB**  
Displays the number of links to the file. For the FAT file systems, this property is always one. For NTFS, it can be more than one.
- **MTIME**  
Displays the time the file was last modified.
- **NAME**  
Displays the file name.
- **OWNER**  
Defines the user or group that owns the record.
- **SACL**  
Windows System Access Control List. Displays audit directives.
- **SIZE**  
Displays the size of the file in bytes.

## GROUP Class (Windows Environment)

The GROUP class contains all group records defined to the Windows operating system. A record in the GROUP class represents every group of users.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Nonmodifiable properties are marked as *informational* and cannot be modified.

- **COMMENT**  
Additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.  
Use the `comment[-]` parameter with the `chgrp`, `editgrp`, and `newgrp` commands to modify this property.  
**Limit:** 255 characters
- **FULL\_NAME**  
The full name associated with a user. Privileged Access Manager uses the full name to identify the user in audit log messages, but not for authorization.  
Use the `name` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.
- **GID**  
(Informational). A value that contains the relative identifier of the group. The accounts database determines the relative identifier when the group is created. It uniquely identifies the group to the account manager within the domain.
- **GLOBAL**  
Indicates a global group. This property is only applicable to Windows groups. This property replaces the `ISGLOBAL` property of earlier Privileged Access Manager versions.  
Use the `global` parameter with the `newgrp (only)` command to add this property.
- **USERLIST**  
The list of users and global groups (for local groups only) that belong to the group. The list that is contained in this property can be different from the one in the Privileged Access Manager database.  
Use the `username(groupname)` parameter with the `join[-]` command to modify this property.
- **PRIVILEGES**  
The Windows rights assigned to the group.  
Use the `privileges` parameter with the `chgrp`, `editgrp`, or `newgrp` command to modify this property.

## OU Class

The OU (Organizational Unit) class contains objects such as user, group, or computer. Objects of class OU can be created on the primary domain controller and could have other objects as child objects (such as group), so an object of class OU is a container object.

### NOTE

The OU class is available only for Windows 2000 Advanced Server with Active Directory installed.

The OU class has no predefined properties (like other classes have). However, you can update the following OU properties:

- Country/Region
- Description
- Desktop
- City
- Display Name
- Folder (Read-only property)
- Fax number
- Managed objects (Read-only property)
- Member of (Read-only property)
- Name (Read-only property)
- Postal address
- Postal code
- P.O. box
- State/Province
- Street
- Telephone
- Object changed (Read-only property)
- Object created (Read-only property)
- Web page

## PRINTER Class

Each record in the PRINTER class defines a device connected to a Windows computer system that is capable of reproducing a visual image on a medium (as listed in Printers folder).

### NOTE

You cannot create new objects of class PRINTER using Privileged Access Manager.

The key of the PRINTER class record is the name of the local printer.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

### • DACL

Defines the standard access control list that contains the user names and group names authorized to access the resource, and the level of access granted to each.

Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).

Each element in the access control list contains the following information:

- **Access Type**

Specifies permissions to the resource:

- a. **Allowed**-Permits special access to the resource.
- b. **Denied**-Denies special access to the resource.

– **Accessor**

The user or group for whom the access rights are allowed or denied.

– **Access**

The access authority that the accessor has to the resource.

**NOTE**

In an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use `auth` or `auth-` command to modify this property.

- **COMMENT**

Defines additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

**Limit:** 255 characters.

- **LOCATION**

A string that indicates the printer location. Privileged Access Manager does not use this information for authorization.

Use the `location` parameter with the `chres` or `editres` commands to modify this property. Use `()` with blanks to delete this property.

- **OWNER**

Defines the user or group that owns the record.

- **SHARE**

The name that identifies the share point for the printer. Users or groups that want to access the printer could use its share name.

Use the `share_name` or `share_name-` parameter with the `chres` or `editres` commands to modify this property.

- **NAME**

Printer name.

- **SACL**

Windows System Access Control List. Displays audit directives.

- **SERVER**

(Informational). A string to identify the server that controls the printer. If there is no such property, the printer is controlled locally.

## PROCESS Class (Windows Environment)

Each record in the PROCESS class defines an object consisting of an executable program, a set of virtual memory addresses, and a thread as listed in the Windows Task Manager.

**NOTE**

You cannot create new objects in the PROCESS class using Privileged Access Manager.

The key of the PROCESS class record is the name of the executable module of the running program.

The following definitions describe the properties contained in this class record. There are no modifiable properties in this class. Non-modifiable properties are marked *informational*.

- **IMAGE\_PATH**

(Informational). The fully qualified path for the specified executable module.

- **PROCESS\_ID**

(Informational). The unique identifier of the process. Process ID numbers are reused, so they identify a process only for the lifetime of that process.



Consider the following limitations when using the PROCESS class:

- Privileged Access Manager traces process creation in Windows. However, seosd fetches new process arguments and writes the arguments to the general trace only if the user who started the process is marked to be traced.
- When a new process is created, its arguments may not be available until the process finishes initialization. seosd attempts to trace the process arguments asynchronously; however if the process is very short, the process may terminate before seosd can fetch the process arguments and write them to the trace. In this case the following message appears in the trace:  
EXECARGS: Not available (87)
- Process IDs are reused in Windows. If a process is very short, it is theoretically possible that seosd will fetch process arguments for a different process that acquired the same process ID, and write these arguments to the trace.

## REGKEY Class (Windows Environment)

Each record in the REGKEY class defines a key in the Windows registry.

The key to the REGKEY record is the full registry path to the Windows registry key.

### NOTE

You can use wildcard characters as part of the path specification.

The following definitions describe the properties contained in a REGKEY record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **DACL**

The standard access control list that contains the user names and group names authorized to access the resource and the level of access granted to each.

Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).

Each element in the access control list contains the following information:

- **Access Type**

Specifies permissions to the resource:

- Allowed**-Permits special access to the resource
- Denied**-Denies special access to the resource

- **Accessor**

The name of the user or group for whom the access rights are allowed or denied.

- **Access**

The access authority the accessor has to the resource. Valid access authorities for the REGKEY class are:

- all**-Allows or denies the accessor to perform all operations permissible for the class
- delete**-Allows or denies the accessor to delete a resource
- read**-Allows or denies the accessor to read the key's contents, but prevents changes from being saved
- rite**-Allows or denies the accessor to change the registry key and its subkeys

### NOTE

It is important to note the differences between an ACL that is empty (that is, one that has no entries) and a resource without an ACL. In the case of an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use auth or auth- command to modify this property.

- **OWNER**

The user or group designated as the owner of the resource.

**NOTE**

Use the owner parameter with the newres, chres, and editres commands to modify this property.

- **SACL**  
Windows System Access Control List specifies audit directives.
- **SUBKEYS**  
(Informational). A list of registry keys (subkeys) located under the key.
- **SUBVALUES**  
(Informational). A list of registry values described in the current registry key.

**REGVAL Class (Windows Environment)**

Each record in the REGVAL class defines data that describes the registry keys. This data stores information necessary to configure the system for one or more users, applications, and hardware devices. Registry values contain information that is constantly referenced during operation. Examples include:

- Profiles for each user
- Applications installed on the computer and the types of files each can create
- Property sheet settings for folders and application icons
- Hardware configuration
- Used ports

The key to the REGVAL record is the full registry key name and its value.

**NOTE**

Changing or deleting registry keys and their values incorrectly can cause serious, system-wide problems that may require you to reinstall Windows to correct them.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Non-modifiable properties are marked *informational*.

- **TYPE**

A format to store data. When you store data under a registry value you can specify one of the following values to indicate the type of data being stored:

**NOTE**

Specify the type when you create or modify the registry value.

- **DWORD**  
Data represented by a number that is four bytes long. Many parameters for device driver and services are this type, and can be displayed in binary, hexadecimal, or decimal format.
- **STRING**  
A sequence of characters representing readable text
- **MULTISTRING**  
A multiple string. Values that contain lists or multiple values in readable text. Entries are separated by null characters.
- **BINARY**  
Raw, binary data. Most hardware component information is stored as binary data and can be displayed in hexadecimal format or in an easy-to-read format.

Use one of these described types as a parameter with the newres, chres or editres to modify this property.

- **VALUE**

The value that the Windows registry value holds.

## SEOS Class (Windows Environment)

The SEOS class controls the behavior of the native local security system.

The class contains only one record, called SEOS, which specifies general native security options. To view or change the status of SEOS class properties, use the `setoptions` command.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **AuditCategory**  
Specifies which detected authorized and unauthorized events are audited.
  - **AccountLogon**  
Specifies whether to audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account.
  - **AccountManagement**  
Specifies whether to audit each event of account management on a computer. Examples of account management events include:
    - A user account or group is created, changed, or deleted.
    - A user account is renamed, disabled, or enabled.
    - A password is set or changed.
  - **DirectoryAccess**  
Specifies whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) defined.
  - **Logon**  
Specifies whether to audit each instance of a user logging on to or logging off from a computer.
  - **ObjectAccess**  
Specifies whether to audit the event of a user accessing an object. For example, a file, folder, registry key, printer, and so on, that has its own system access control list (SACL) defined.
  - **PolicyChange**  
Specifies whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies.
  - **PrivilegeUse**  
Specifies whether to audit each instance of a user exercising a user right.
  - **DetailedTracking**  
Specifies whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.
  - **System**  
Specifies whether to audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.
- **History**  
Defines the number of unique new passwords that have to be associated with a user account before an old password can be reused.  
**Limits:** An integer between 1 and 24. If you specify zero, no passwords are saved.
- **Interval**  
Defines the period of time (in days) that a password can be used before the system requires the user to change it.
- **Min life**  
Defines the period of time (in days) that a password must be used before the user can change it.
- **Min length**  
Defines the least number of characters that a password for a user account may contain.
- **Password fails**

Defines the number of failed logon attempts that causes a user account to be locked out.

- **Reset count after**

Defines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts.

## SERVICE Class

Each record in the SERVICE class defines a Windows service as listed in the Windows Control Panel, Services.

The key of the SERVICE class record is the name of the service being controlled.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **ACCOUNT**

Changes the login account for the service. Although most services must log in to the system account, some services can be configured to log in to special user accounts. For more information, see the relevant Microsoft Windows documentation. The default value is `LocalSystem`.

Use the `account` parameter with the `chres` or `editres` commands to modify this property.

- **BINARY\_NAME**

The full path which points to the location of the service's executable.

- **IMAGEPATH**

The fully qualified path for the specified executable module.

- **INTERACTIVE**

Provides a user interface on the desktop that can be used by whoever is logged in when the service is started. This is available only if the service is running as a `LocalSystem` account.

Use the `interactive` parameter with the `chres` or `editres` commands to modify this property.

- **PROFILE**

A string that specifies the path to the user's profile. This string can include a local absolute path, or a UNC path.

Use the `profile` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

- **REG\_KEY**

This property points to the location of the service definition in Windows registry.

- **STARTUPTYPE**

Defines how (when) the service is started. Options are:

- **automatic**-Starts automatically during system startup.
- **disabled**-Prevents users or dependent services from starting the service.
- **manual**-Allows the service to be started by a user or a dependent service.
- Use the `startuptype` parameter with the `chres` or `editres` commands to modify this property.

- **STATUS**

Changes the current service state. Options are: `started`, `stopped`, and `paused`.

Use the `status` parameter with the `chres` or `editres` commands to modify this property.

### Example: Configure a service to start manually

To change the service `SeOSAgent` to start manually, enter the `selang` command:

```
chres SERVICE "SeosAgent" starttype(manual)
```

### Example: Change a directory login account

To change the login account of the Directory Replicator to `ReplAdmin` with password `abcde`, enter the `selang` command:

```
chres SERVICE directory replicator account(repladmin) domainpwd(abcde)
```

## SESSION Class

Each record in the SESSION class defines a user session on the local host. The record includes the user name, computer name, elapsed time of the connection, and the resources being used.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **CNAME**  
The host name where the session was established.
- **GUEST**  
Indicates whether the session was created on Guest account.
- **IDLE**  
Ends a network session between a server and a workstation.  
Use the `disconnect` parameter with the `chres` or `editres` commands to modify this property.
- **OPENS**  
Indicate the number of open sessions.
- **RESOURCES**  
A property that gives information about shared files on a server. This information includes the path of the opened shared resource and the user or computer that opened the resource.
- **TIME**  
The time elapsed since the session was established.
- **USER**  
A value that contains the relative ID (RID) of the user. The RID is determined by the Security Account Manager (SAM) when the user is created. It uniquely defines the user account to SAM within the domain.

### Example: Disconnect a user from a local session

To disconnect user ZORRO from a session on the local host, enter the `selang` command:

```
chres SESSION zorro disconnect
```

#### NOTE

Disconnecting users may result in loss of data. It is a good idea to warn connected users before disconnecting them.

## SHARE Class

Each record in the SHARE class defines a share resource that could be any device, data, or program used by one or more devices or programs. For Windows, shared resources refer to any resource that is made available to network users, such as directories, files, printers, and named pipes. A share also refers to a resource on a server that is available to network users.

The key of the SHARE class record is the share name of the resource.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using `selang` or the administration interfaces. Non-modifiable properties are marked *informational*.

- **CURR\_USERS**  
(Informational). The number of current connections to the resource.
- **DACL**  
Defines the standard access control list that contains the user names and group names authorized to access the resource, and the level of access granted to each.  
Users who want to modify this property must be the owner of the resource or have special access to the resource (to modify the ACL).  
Each element in the access control list contains the following information:

- **Access Type**

Specifies permissions to the resource:

- Allowed**-Permits special access to the resource.
- Denied**-Denies special access to the resource.

- **Accessor**

The user or group for whom the access rights are allowed or denied.

- **Access**

The access authority that the accessor has to the resource.

**NOTE**

In an empty ACL, no accesses are explicitly granted, so access is implicitly denied. For a resource that has no ACL, no protection is assigned to the object, so any access request is granted.

Use `auth` or `auth-` command to modify this property.

- **MAX\_USERS**

The maximum number of concurrent connections that the shared resource can accommodate.

**NOTE**

You cannot supply zero (0) as a value for this property. Windows ignores it.

Use the `max_users` parameter with the `newres`, `chres`, or `editres` commands to modify this property.

- **NAME**

Defines the name of the share.

**NOTE**

PATH

A string that specifies a local path for the shared resource. For disks, this is the path being shared. For print queues, this is the name of the print queue being shared.

Use the `path` parameter with the `newres`, `chres`, or `editres` commands to modify this property.

- **PERMISSION**

(Informational). A value that indicates the shared resource's permissions for servers running with share-level security. This property can be any of the values in the following table:

- **ACCESS\_READ**

Permission to read data from a resource and, by default, to execute the resource.

- **ACCESS\_WRITE**

Permission to write data to the resource.

- **ACCESS\_CREATE**

Permission to create an instance of the resource (such as a file); data can be written to the resource as the resource is created.

- **ACCESS\_EXEC**

Permission to execute the resource.

- **ACCESS\_DELETE**

Permission to delete the resource.

- **ACCESS\_ATTRIB**

Permission to modify the resource's attributes (such as the date and time when a file was last modified).

- **ACCESS\_PERM**

Permission to modify the permissions (read, write, create, execute, and delete) assigned to a resource for a user or application.

- **ACCESS\_ALL**

Permission to read, write, create, execute, and delete resources, and to modify their attributes and permissions.

- **ACCESS\_NONE**

Denies permissions.

- **REMARK**

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. Privileged Access Manager does not use this information for authorization.

Use the comment or comment- parameter with the newres, chres, or editres commands to modify this property.

- **RESOURCES**

(Informational). A property that gives information about shared files on a server. This information includes the path of the opened shared resource and the user or computer that opened the resource.

- **TYPE**

(Informational). The type of share. Use one of the following types for a shared resource:

- **File Folder**

A disk drive. This can also refer to remote administration of the server (ADMIN\$) and to administrative shares such as C\$, D\$, and so on.

- **Print Queue**

A print queue

- **Communication device**

A communication device

- **Interprocess Communication (IPC)**

A special share reserved for interprocess communication (IPC\$)

- **USERS**

Information about users currently accessing the shared resource. This information includes the name of user who made the connection (USER), the share name of the server's shared resource, or the computer name of the client (MACHINE). It also includes the number of seconds that the connection has been established (TIME) and the number of files currently open as a result of the connection (INUSE).

## USER Class (Windows Environment)

The USER class contains all user records defined to the Windows operating system. The key of the USER record is the name of the user, which is the name that the user entered when logging in to the system.

The following definitions describe the properties contained in this class record. Most properties are modifiable and can be manipulated using selang or the administration interfaces. Nonmodifiable properties are marked *informational*.

- **BAD\_PW\_COUNT**

(Informational). The number of times the user tried to log in to the account using an incorrect password. A value of -1 indicates that the value is unknown.

- **COMMENT**

Additional information that you want to include in the record. Privileged Access Manager does not use this information for authorization.

Use the comment[-] parameter with the chusr, editusr, and newusr commands to modify this property.

**Limit:** 255 characters.

- **COUNTRY**

A string that specifies a country descriptor for a user. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.

Use the country parameter with the chusr, editusr, and newusr commands to modify this property.

- **DAYTIME**

The day and time restrictions that govern when a user can access the resource.

Use the restrictions parameter with the chusr, editusr, and newusr commands to modify this property.

**Note:** The information in this property is identical to the information in the DAYTIME property in the AC environment. However, any minute value that is entered is truncated.

- **DIAL\_CALLBACK**

The type of call-back privileges provided to the user. The following options are defined:

- **NoCallback**

The user has no call-back privileges.

- **SetByCaller**

The remote user can specify a call-back phone number when dialing in.

- **Call-back Phone Number**

The administrator sets the call-back number.

Use the `gen_prop` or `gen_val` parameters with the `chusr` or `editusr` command to modify this property.

- **DIAL\_PERMISSION**

Permission to dial in to the RAS server. When you specify 0 as value, the user cannot dial in to the RAS server.

Use the `gen_prop` or `gen_val` parameter with the `chusr` or `editusr` command to modify this property.

- **EXPIRE\_DATE**

The date on which a USER record expires and becomes invalid. A value for the EXPIRE\_DATE property in a USER record overrides a value in a GROUP record. To reinstate the expired record, use the `chusr` command with the `expire-` parameter. You cannot resume an expired user. You can resume a suspended user by specifying a resume date.

Use the `expire` or `expire-` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

- **FLAGS**

Flags that you can assign to the account of a user to specify particular attributes. You can apply more than one flag to each account.

Use the `flags` parameter with the `chusr`, `editusr`, and `newusr` commands to modify this property.

- **FULL\_NAME**

The full name associated with a user. Privileged Access Manager uses the full name to identify the user in audit log messages, but not for authorization.

Use the `name` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

- **GID**

A value that contains the relative identifier of the group. The accounts database determines the relative identifier when the group is created. The relative identifier uniquely identifies the group to the account manager within the domain.

- **GROUPS**

The list of groups a user belongs to. The group list that is contained in this property can be different from the one in the AC environment GROUPS property.

Use the `group` parameter with the `join[-]` command to modify this property.

- **HOME**

The home directory is the folder that is accessible to the user and contains files and programs for that user. The home directory can be assigned to an individual user or can be shared among many users.

- **HOMEDIR**

A string specifying the home directory of a user. Users log in to their home directories automatically.

Use the `homedir` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

- **HOME\_DRIVE**

A string that specifies the drive of the home directory of a user. Users log in to their own home drives and home directories automatically.

Use the `homedrive` parameter with the `chusr`, `editusr`, or `newusr` command to modify this property.

- **ID**

A value that contains the relative ID (RID) of the user. The Security Account Manager (SAM) determines the RID when the user is created. The RID uniquely defines the user account to SAM within the domain.

- **LAST\_ACC\_TIME**

(Informational). The date and time of the last login.

- **LAST\_LOGOFF**

(Informational). The date and time of the last logoff.

- **LOCATION**

A string that is used to store a user location. Privileged Access Manager does not use this information for authorization.

Use the `location` parameter with the `chusr`, `editusr`, and `newusr` commands to modify this property.

- **LOGON\_SERVER**



A string that specifies the server that verifies the login information for the user. When the user logs in to the domain workstation, Privileged Access Manager transfers the login information to the server. The server gives the workstation permission for the user to work.

- **MAX\_LOGINS**  
(Informational). The number of times the user logged in successfully to this account. A value of -1 indicates that the value is unknown.
- **NAME**  
The name of the user.
- **ORGANIZATION**  
A string that stores information on the organization in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.  
Use the organization parameter with the chusr, editusr, and newusr commands to modify this property.
- **ORG\_UNIT**  
A string that stores information about the organizational unit in which the user works. This string is part of the X.500 naming scheme. Privileged Access Manager does not use it for authorization.  
Use the org\_unit parameter with the chusr, editusr, and newusr commands to modify this property.
- **PASSWD\_EXPIRED**  
Expiration date for the user account.
- **PGROUP**  
A user's primary group ID. A primary group is one of the groups in which a user is defined. A primary group must be a global group. This string cannot include spaces or commas.  
Use the pgroup parameter with the chusr, editusr, or newusr command to modify this property.
- **PHONE**  
A string that can be used to store a user telephone number. This information is not used for authorization.  
Use the phone parameter with the chusr, editusr, and newusr commands to modify this property.
- **PRIVILEGES**  
The Windows rights assigned to the user.  
Use the privileges parameter with the chusr, editusr, or newusr command to modify this property.
- **PROFILE**  
A string that specifies a path to the profile of the user. This string can include a local absolute path, or a UNC path.  
Use the profile parameter with the chusr, editusr, or newusr command to modify this property.
- **PW\_LAST\_CHANGE**  
(Informational). The date and time on which the password was updated.
- **RESUME\_DATE**  
The date on which a suspended USER account becomes valid.  
See SUSPEND\_DATE for an explanation of how RESUME\_DATE and SUSPEND\_DATE work together.
- **SCRIPT**  
A string that specifies the path for the logon script file of the user. The script file can be a .CMD, .EXE, or .BAT file.
- **TERMINALS**  
A string that specifies a list of terminals from which the user can log in.  
Use the terminals parameter with the chusr, editusr, and newusr commands to modify this property.
- **TS\_CONFIG\_PGM**  
A value that indicates whether the client can specify the initial program.  
The TS\_INITIAL\_PGM user property indicates the initial program. If you specify the initial program of a user, it becomes the only program that user can run. The terminal server logs off the user when the user exits that program. When this value is set to 1, the client can specify the initial program. When this value is set to 0, the client cannot specify the initial program.  
Use the gen\_prop and gen\_val parameters with the chusr and editusr commands to modify this property.
- **TS\_HOME\_DIR**  
The path of the home directory of the user for terminal server logon. This string can specify a local path or a UNC path (\\machine\share\path).

Use the `gen_prop` and `gen_val` parameters with the `chusr` and `editusr` commands to modify this property.

- **TS\_HOME\_DRIVE**

A drive specification (a drive letter followed by a colon) to which the UNC path is specified in the `TS_HOME_DIR` property.

Use the `gen_prop` and `gen_val` parameters with the `chusr` and `editusr` commands to modify this property.

- **TS\_INITIAL\_PGM**

The path of the initial program that Terminal Services runs when the user logs on.

If you specify the initial program of a user, that is the only program that user can run. Terminal server logs off the user when the user exits that program.

When `TS_CONFIG_PGM` property is set to 1, the client can specify the initial program.

Use the `gen_prop` and `gen_val` parameters with the `chusr` and `editusr` commands to modify this property.

- **TS\_PROFILE\_PATH**

The path of the profile of the user for terminal server logon. The directory that is identified by the path must be created manually and must exist before the logon.

Use the `gen_prop` and `gen_val` parameters with the `chusr` and `editusr` commands to modify this property.

- **TS\_WORKING\_DIR**

The path of the working directory for the initial program that Terminal Services runs when the user logs on.

Use the `gen_prop` and `gen_val` parameters with the `chusr` and `editusr` commands to modify this property.

- **WORKSTATIONS**

A list of the workstations from which the user can log in.

Use the `workstations` parameter with the `chusr`, `editusr`, and `newusr` commands to modify this property.

## Classes in the UNIX Environment

This section contains a complete alphabetic reference to all the UNIX classes that exist in the UNIX system files (classes in the unix environment). The properties for these native classes are governed by the operating system and vary between systems.

### NOTE

The term *unix environment* refers to the system files accessed with the `selang` command `env unix`. These are the same system files the UNIX operating system maintains for users and groups and the files on the system.

Use the table of contents to access the topics in this section.

### FILE Class (UNIX Environment)

Each record in the FILE class defines a file located on a physical or logical drive of a computer on a file system.

### NOTE

You cannot create files physically on disk using Privileged Access Manager.

The key of the FILE class record is the name of the file or directory protected by the record. The full path must be specified.

The properties for the this native class are governed by the operating system and vary between systems. The `chfile` command lists the native properties you can modify using `selang`.

### GROUP Class (UNIX Environment)

The GROUP class contains all group records defined to the UNIX operating system. A record in the GROUP class represents every group of users.

The properties for the this native class are governed by the operating system and vary between systems. The `chgrp` command lists the native properties you can modify using `selang`.

## USER Class (UNIX Environment)

The USER class contains all user records defined to the UNIX operating system. The key of the USER record is the user's name, which is the name entered by the user when logging into the system.

The properties for the this native class are governed by the operating system and vary between systems. The `chusr` command lists the native properties you can modify using `selang`.

## Classes for Custom Purposes

This section contains user defined classes and properties.

**Use the table of contents to access the topics in this section**

### User Defined Class

Each record in the User Defined class defines access to a custom-made class that meets your own needs. The only restriction on the name of user-defined classes is that the name cannot be all uppercase letters.

The key of a User Defined class record is the name of the record.

## Windows Values for PAM SC `selang` Commands

This section contains information about Windows values for PAM SC `selang` commands.

**Use the table of contents to access the topics in this section.**

## File Attributes

Attributes can be assigned to a file by using the `chfile`, `editfile`, and `newfile` commands. Attributes determine the character of the file.

### NOTE

Although the full name for these file attributes is `FILE_ATTRIBUTE_name`, Privileged Access Manager only requires you to enter the *name* portion (for example, `ARCHIVE` or `COMPRESSED`).

The following lists and describes the file attributes that you can modify in Windows.

- **FILE\_ATTRIBUTE\_ARCHIVE**  
An archival file; a file marked for backup or removal.
- **FILE\_ATTRIBUTE\_HIDDEN**  
A hidden file. Hidden files are not normally included in an ordinary directory listing.
- **FILE\_ATTRIBUTE\_NORMAL**  
A file with no other attributes. This value is only valid when used alone.
- **FILE\_ATTRIBUTE\_READONLY**  
A read-only file. Applications can read the file, but cannot write in it or delete it.
- **FILE\_ATTRIBUTE\_SYSTEM**  
An operating system file or a file used exclusively by the operating system.
- **FILE\_ATTRIBUTE\_TEMPORARY**  
A file being used for temporary storage.

The following lists and describes the file attributes that you cannot modify in Windows.

- **FILE\_ATTRIBUTE\_COMPRESSED**

A compressed file or directory. For files, this means all the data in the file is compressed; for directories, this means that all newly created files and subdirectories are compressed by default.

- **FILE\_ATTRIBUTE\_DIRECTORY**

A directory.

## Account Flags

Flags can be assigned to a user's account to specify particular attributes of that account by using the `chusr`, `editusr`, and `newusr` commands. You can apply more than one flag to each account.

### NOTE

You do not need to enter the complete name of the flag. You can use the shortcuts provided in the table.

Following are the account flags available in Windows.

Shortcut	Flag	Description
blank	UF_PASSWRD_NOTREQD	Indicates that no password is required for the user's account.
cant_change	UF_PASSWORD_CANT_CHANGE	Indicates that the user cannot change the password for the account.
disable	UF_ACCOUNTDISABLE	Indicates the user's account is disabled.
dont_expire	UF_DONT_EXPIRE_PASSWORD	Indicates that the password for this account never expires.
homedir	UF_HOMEDIR_REQUIRED	Indicates the home directory is required. This value is ignored in Windows.
interdomain	UF_INTERDOMAIN_TRUST_ACCOUNT	Indicates a permit to trust account.
lockout	UF_LOCKOUT	Indicates that the user's account is currently locked out; to unlock a locked account, remove this flag
normal	UF_NORMAL_ACCOUNT	Indicates a default account type that represents a normal user.
notreq	UF_PASSWRD_NOTREQD	Indicates that no password is required for the user's account.
protect	UF_PASSWORD_CANT_CHANGE	Indicates that the user cannot change the password for the account.
script	UF_SCRIPT	Indicates that the login script, which executes disk mapping, is activated when the user starts an application. This flag must be set for LAN Manager 2.0 or Windows.
server	UF_SERVER_TRUST_ACCOUNT	Indicates an account for a Windows NT Backup Domain Controller in this domain.
temp	UF_TEMP_DUPLICATE_ACCOUNT	Indicates a user with an account in another domain; provides access to the domain for this account, but not a trust account.
trust	UF_INTERDOMAIN_TRUST_ACCOUNT	Indicates a permit to trust account.
workstation	UF_WORKSTATION_TRUST_ACCOUNT	Indicates an account for a workstation or server that is a member of this domain.

## Permissions

In the SHARE resource type, you can give access permissions to accessors.

Following are the access permissions available in Windows:

- **ACCESS\_ALL**  
Permission to read, write, create, execute, and delete resources and to modify their attributes and permissions.
- **ACCESS\_ATTRIB**  
Permission to modify the resource's attributes.
- **ACCESS\_CREATE**  
Permission to create a resource, including writing data to it as it's being created.
- **ACCESS\_DELETE**  
Permission to delete the resource.
- **ACCESS\_EXEC**  
Permission to execute the resource.
- **ACCESS\_NONE**  
No access.
- **ACCESS\_PERM**  
Permission to modify the permissions assigned to a user or an application for a resource.
- **ACCESS\_READ**  
Permission to read data from a resource and, by default, to execute in the resource.
- **ACCESS\_WRITE**  
Permission to write data to the resource.

## Privileges

Windows privileges can be assigned to individual user accounts and groups. Administrators can assign privileges to a user with the `chusr` or `editusr` command, or to a group with the `chgrp` or `editgrp` command. Users who are added to a group automatically gain all the privileges assigned to the group.

You can use the name of the privilege, or user right, exactly as it appears in the list, or you can add `Se` to the beginning and `Privilege` to the end of the name (except for `BatchLogon`, `InteractiveLogon`, `NetworkLogon`, and `ServiceLogon`, to which you add `Right` instead of `Privilege`).

Following are the privileges available in Windows.

Privilege	Default Assignment	Description
AssignPrimaryToken	None	Allows a user to modify the security access token of a process.
Audit	None	Generates security audits.
Backup	Administrators Backup Operators	Allows a user to back up files and directories. This privilege replaces all file and directory permissions.
BatchLogon	None	Allows a user to log in as a batch job.

ChangeNotify	Everyone	Usually, rights to files and subdirectories flow downward; that is, users who do not have rights to a specific directory do not also have rights to access the subdirectories below that directory. This privilege allows a user to access subdirectories, even if that user has no rights to the parent directories.
CreatePagefile	None	Allows a user to create a page file. Security is determined by a user's access to the key: \CurrentControlSet\Control\SessionManagement
CreatePermanent	None	Allows a user to create special permanent objects, such as \\Device
CreateToken	None	Creates a token object. Only the Local Security Authority can do this. The Local Security Authority ensures that the user has permission to access the system. It is not possible to audit the use of this right. For C2 certification, we recommend that it not be assigned to any user.
Debug	Administrator	Debugs programs or objects such as threads. You cannot audit this privilege. For C2 certification, we recommend that it not be assigned to any user, including system administrators.
IncreaseBasePriority	Administrators PowerUsers	Allows a user to increase the execution priority of a process.
IncreaseQuota	None	Allows a user to increase the object quotas.
InteractiveLogon	Most groups	Allows the user to log in interactively.
LoadDriver	Administrators	Allows a user to install and remove device drivers.
LockMemory	None	Allows a user to lock pages in the memory of the computer so the pages cannot be automatically backed up on a backing store like PAGEFILE.SYS.
MachineAccount	None	Allows a user to add a new machine to a domain.
NetworkLogon	Everyone	Allows users to connect to a computer from anywhere in the network. This means users do not have to be at a specific place or terminal to log into their computer.
ProfileSingleProcess	Administrators PowerUsers	Allows a user to use performance-monitoring tools in order to monitor the performance of a single process.
RemoteShutdownPrivilege	Administrators PowerUsers	Allows a user to shut down a Windows system remotely.
Restore	Administrators Backup Operators	Allows a user to restore backed-up files and directories. This right replaces all file and directory permissions.

Security	Administrators	Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. <b>Note:</b> This privilege does not allow the user to set system auditing policies using the Audit command from the Policy menu in Microsoft's User Manager. Administrators always have the ability to view and clear the security log.
ServiceLogon	None	Enables a process to register with the system as a service.
Shutdown	Administrators BackupOperators Everyone PowerUsers Users	Allows the user to shut down the system from the system console.
SystemEnvironment	Administrators	Allows a user to modify the system environment variables. This enables the user to set up the system environment at their workstation, and ensure that all other users working on the same workstation use the same setup.
SystemProfile	Administrators	Allows a user to perform profiling (performance sampling) on the system.
SystemTime	Administrators Power Users	Allows a user to set the time for the internal clock of the computer.
TakeOwnership	Administrators	Allows a user to become the owner of files, directories, printers, and other objects on the computer. This right replaces all permissions protecting objects.
Tcb	None	Enables a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this privilege.

## String Matching

This section describes the syntax that can be used to build wildcard expressions.

Privileged Access Manager performs string matching (globbing) using the wildcard matching and character lists.

## Examples Wildcard Matching

To make a single character a don't care character that matches any other single character, use a question mark (?):

Specify	To match
mmc?	mmc3, mmcX, mmc5
mmc?.t	mmc1.t, mmc2.t
mmc04.?	mmc04.a, mmc04.1

To match any string of zero or more characters, use an asterisk (\*):

Specify	To match
*i*.c	main.c, list.c, and so on

st*.h	stdio.h, stdlib.h, string.h, and so on
*	All records of the specified class

To match any character in a list, follow one of these examples:

Specify	To match
[abcgk]	a, b, c, g, or k
[^abcgk]	Any character other than a, b, c, g, or k, such as A, B, d, e, f, or @.
[a-z]	Any character between a and z, inclusive.
[^a-z]	Any character with an ASCII value less than a or greater than z.
[Z-]	Any character with an ASCII value greater than Z's, such as a, b, \, or ~.
[^A]	Any character with an ASCII value <i>not</i> lower than A's, such as B, a, c, or ~.

## Character Lists

A character list that is enclosed by square brackets ( [ ] ) can contain one or more characters. Privileged Access Manager uses these characters as positive or negative matching criteria.

A character list can be composed of one or more characters. For this type of list, Privileged Access Manager matches any single character in the list. If the list within the brackets is preceded by a caret (^), Privileged Access Manager matches any single character, which is *not* in the list.

A range is a type of character list that specifies a range of characters. Privileged Access Manager matches all the characters in the list, inclusively. If a caret (^) precedes the list, Privileged Access Manager excludes all the characters in the specified list. You can specify both ends of the range, or only its first or last character.

The following table describes the character lists that can be used. In this syntax, include the square brackets. Each of the expressions *ch1*, *ch2*, and *chN*, stands for a single character.

List	Matches
[ <i>ch1ch2...chN</i> ]	Any single character in the list enclosed by the square brackets
[^ <i>ch1ch2...chN</i> ]	Any single character that is <i>not</i> in the list enclosed by the square brackets
[ <i>ch1-ch2</i> ]	Any single character in the range, inclusive
[^ <i>ch1-ch2</i> ]	Any single character that is <i>not</i> in the inclusive range
[ - <i>ch2</i> ]	Any single character with an ASCII value lower than or equal to the specified character ( <i>ch2</i> )
[ ^ - <i>ch2</i> ]	Any single character with an ASCII value equal to or higher than the specified character ( <i>ch2</i> )
[ <i>ch1</i> - ]	Any single character with an ASCII value equal to or higher than the specified character ( <i>ch1</i> )
[ ^ <i>ch1</i> - ]	Any single character with an ASCII value equal to or lower than the specified character ( <i>ch1</i> )



## Registry

Privileged Access Manager creates its registry entries under the following registry key, which is called ACROOT in Privileged Access Manager Endpoint Management Remote Configuration:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
```

The main registry key contains the following registry entries:

- **CurrentVersion**  
Defines the current version and build of product.
- **Encryption Package**  
Defines the full path name of the DLL used to implement symmetric encryption.  
**Default:** *ACInstallDir\bin\aes256enc.dll*

## Build Number

Privileged Access Manager defines the current version and build of product in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Build_Number
```

This key is for internal use only.

## AccessControl

Privileged Access Manager maintains generic settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl
```

The AccessControl registry key contains the following registry entries:

- **AccessControl Services**  
Defines a list of Privileged Access Manager service names and the executable.  
**Default:** "SeOSAgent;SeOS Agent", "SeSudo;SeOS TD", "seoswd;SeOS Watchdog"  
**Note:** The endpoint that is part of the Enterprise Management Server also contains the following default values for this registry entry: "Sepmdd;SeOS Policy Model(DMS\_\_)", "Sepmdd;SeOS Policy Model(DH\_\_)", "Sepmdd;SeOS Policy Model(DH\_\_WRITER)"
- **admin\_default\_check**  
Specifies whether Privileged Access Manager is denied login access to the Privileged Access Manager server, even when the *defaccess* property for a remote terminal resource is set to *all*, or access to *\_default* terminal resource is permitted.  
Maintained for backward compatibility.  
**Default:** 0 (access is not denied)
- **AdminInst**  
Internal use only.  
**Default:** 0
- **auth\_login**  
Specifies how a user is authenticated for administration purposes.  
Valid values are:  
**native** - for native operating system users, checks the user password against OS.  
**eTrust** - for users that do not exist in the native operating system, checks the user password against Privileged Access Manager database.  
**Default:** native
- **auth\_module\_names**

The list of the language client modules that are allowed to authenticate outside of native authentication. Client module name is set by the client inside the lca API calls before the authentication. Changing this registry value can affect other clients authenticating in a nonnative mode.

**Default:** none

- **CPF\_TARGETS**

List of target mainframe CPF systems (remote CPF target nodes) that the CPF service communicates with.

**Default:** ACF2 TOP RACF

- **eACPipePrefix**

A value for part of the pipe name that the new pipe servers and pipe clients use. If a system has older clients of Privileged Access Manager, then this value is obligatory for those clients to work. Otherwise, change this value to a more secure pipe name.

**Default:** SEOS

- **eACPipeTranslator**

Obsolete.

- **full\_year**

Specifies whether years appear in two-digit (value=no) or four-digit (value=yes) format, when using the secons -tv, seaudit, and dbmgr utilities.

**Default:** yes

- **GenerateMemDump**

Specifies whether Privileged Access Manager creates a memory dump (1) when handling a code exception of a Privileged Access Manager service. Privileged Access Manager creates the memory dump in *ACInstallDir\bin\serviceProcessName.PID.dmp* Example: SeOSAgent.5704.dmp

**NOTE**

The memory dump is only for user mode and not kernel mode.

**Default:** 1

- **parent\_pmd**

The PMDB to which this workstation subscribes in the format of *pmdb@host*. This is the only policy model that can update the local database.

If you do not specify a value, the workstation does not accept updates from any PMDB. If you set the entry to *\_NO\_MASTER\_*, then any PMDB can update this workstation

No default.

**Example:** pmd1@host1;pmd2@host1;pmd3@host2

- **passwd\_pmd**

The target for password replacement on the policy model in the format *pmdb@host*.

The parent\_pmd and passwd\_pmd registry values can have the same value. If the parent\_pmd and passwd\_pmd registry values are not the same, the passwd\_pmd database sends its updates to the parent\_pmd database for distribution. The parent\_pmd database must be a subscriber of the passwd\_pmd database.

If you do not set this value, it inherits the value of the parent\_pmd registry key.

No default.

- **ReverseIpLookup**

Controls the way the client IP address is resolved to determine whether the user is allowed to log in from that terminal.

Valid values are:

**yes**-looks up the IP address of the open client's socket and logon is permitted accordingly.

**no**-uses the host name as received from the client and does not resolve any host names. (The same effect can be achieved by disabling class *TERMINAL*.)

**Default:** yes

- **secondary\_pmd**

Specifies the PMDB used as the secondary target for password replacement for users who are not defined in the primary target (passwd\_pmd).

The format is *pmd\_name@hostname*.

No default.

- **SeOSPath**  
The directory in which Privileged Access Manager is installed.
- **SplashEnable**  
The toggle to enable or disable a protection message during interactive (GINA) login process. This message tells the user that Privileged Access Manager protects the computer. A value of 1 indicates that the message is enabled; a value is 0 indicates that it is disabled.  
**Default:** 1
- **TrustedServices**  
List of trusted programs.  
No default.
- **UseFsiDrv**  
Toggle to enable or disable driver loading.  
**Values:** 1 - Enable driver loading, 0 - Disable driver loading  
**Default:** 1

## agent

Privileged Access Manager maintains agent settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Agent
```

Agent key entries (and any subkeys) are for internal use only.

- **ShutdownWaitingTimeout**  
Defines the timeout period, in milliseconds, the Privileged Access Manager Agent waits for its components to gracefully shut down. If Privileged Access Manager components do not shut down gracefully, the Agent shuts down forcefully.  
**Note:** This registry entry is for internal use only.  
**Default:** 60000

## Applications

Privileged Access Manager maintains application settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications
```

The Applications registry key contains the following registry entries:

- **OperationMode**  
Specifies whether the controlled application mode is active (1).  
Set this value to 1.  
**Default:** 1

## Application Name

Privileged Access Manager maintains specific application settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications\Application_Name
```

Each Applications\*Application\_Name* registry key contains the following registry entries:

- **ApplicationName**  
Defines the name of controlled process.  
You must specify the full pathname in this format: *device:\path\name.exe*.

**Default:** Full pathname to executable

- **Arguments**  
Defines arguments Privileged Access Manager uses when starting the application.  
**Default:** "" (no arguments)
- **Desktop**  
Defines the workstation and session name.  
**Default:** No default
- **OperationMode**  
Specifies whether the application is active (1).  
**Default:** 1
- **RestartApplication**  
Specifies whether the application will be restarted (1) if it has been closed or terminated.  
**Default:** 1
- **StartApplication**  
Specifies whether Privileged Access Manager be starts the application (1) when the Watchdog wakes up.  
**Default:** 1
- **WorkingDirectory**  
Defines the working directory in which the application is started.  
**Default:** *ACInstallDir\bin*

## Client

Privileged Access Manager maintains client application settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client
```

The Client registry key contains the following registry entries:

- **ConnectTo**  
Defines the host name Privileged Access Manager client administration applications (for example, selang) connect to by default.  
**Default:** localhost

## standalone

Privileged Access Manager maintains standalone client settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client\Standalone
```

The Client\Standalone registry key contains the following registry entries:

- **full\_login\_check**  
The toggle to enable the Privileged Access Manager server to check additional user properties (grace and max\_login) and perform a login during a connection request from a standalone application.  
This value helps remote password changes if one is about to expire.  
If the value is set to 1, the checks are enabled.  
**Default:** 0

## Common

Privileged Access Manager maintains settings used by common components under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common
```

The Common key does not contain any registry entries. It contains registry subkeys for common components.

## AgentManager (Windows)

Privileged Access Manager maintains the Agent Manager related settings in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager
```

The Agent Manager registry key contains the following registry entries:

- **RefreshTimeout**  
Defines the Agent Manager refresh interval, in seconds.  
**Type:** REG\_DWORD  
**Default:** 600
- **StandAloneService**  
Specifies whether or not this service is a standalone service.  
**Type:** REG\_DWORD  
**Default:** 0
- **TraceEnabled**  
Defines the Privileged Access Manager Agent Manager trace mode.  
**Values:** 0,1  
**Default:** 1
- **TraceFileSize**  
Defines the maximum log files size.  
**Type:** REG\_DWORD  
**Default:** 20MB
- **Workspace**  
Specifies the full pathname of the Privileged Access Manager Agent Manager workspace.  
**Default:** ACInstallDir\Data\AgentManager

## Plugins

Privileged Access Manager maintains settings that are used by the plugins under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
```

The Plugins key does not contain any registry entries. It contains registry subkeys for plugins.

## AccountManager

Privileged Access Manager maintains the Account Manager related settings in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager\Plugins  
\AccountManager
```

The Account Manager registry key contains the following registry entries:

- **ComponentName**  
Specifies the name of the AgentManager plug-in.
- **Exclude\_Endpoint\_Types**  
Defines the endpoints types that the current AccountManager does not process.  
**Values:** A comma separated list of endpoint types.  
**Example:**

```
exclude_endpoint_types = Windows Agentless
```

- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 1  
**Note:** Applicable only when ScheduleType is set to 2.
- **JCS\_add\_timeout**  
Specifies JCS timeout in seconds during an *add* operation.  
**Default:** 300
- **JCS\_modify\_timeout** Specifies JCS timeout in seconds during a *modify* operation.  
**Default:** 300
- **JCS\_search\_timeout** Specifies JCS timeout in seconds during a *search* operation.  
**Default:** 300
- **max\_threads\_count**  
Defines the number of working threads in the pool.  
**Values:** 50  
**Type:** REG\_DWORD
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 0
- **PluginPath**  
Defines the full pathname of the plugin.  
**Type:** REG\_SZ  
**Default:** \ProgramFiles\CA\PAMSCServer\APMS\PAMSC\bin\AccountManager.dll
- **QueryFilter**  
Specifies additional values that are added to the Message Queue receive queue filter.  
**Options:** ENDPOINT\_CUSTOM 1...5=, ENDPOINT\_OWNER=, ENDPOINT\_DEPARTMENT=

#### NOTE

- Place property values in apostrophes
- Use AND and OR operands to specify more than a single property
- Use parenthesis when needed

- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

#### NOTE

Applicable only when ScheduleType is set to 2.

- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 1
- **wmi\_timeout**  
Defines in seconds how long WMI waits for a response from the endpoint before timeout.  
**Default:** 60

### PupmAgentManager

Privileged Access Manager maintains the PupmAgentManager related settings in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
\PupmAgent
```

The PupmAgentManager registry key contains the following registry entries:

- **AutoRegister**  
Defines the auto registration interval in days.  
**Default:** 7
- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 1  
**Note:** Applicable only when ScheduleType is set to 2.
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 0
- **PluginPath**  
Defines the full pathname of the plugin.  
**Default:** /opt/CA/PAMSCShared/lib/AccountManager.so
- **RegistrationInterval**  
Specifies the registration schedule in intervals.  
**Default:** 7  
**Type:** REG\_DWORD
- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat  
  
**NOTE**  
Applicable only when ScheduleType is set to 2.
- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 1

### **DiscoveryAgent**

Privileged Access Manager maintains settings that are related to the DiscoveryAgent in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
\DiscoveryAgent
```

The DiscoveryAgent registry key contains the following registry entries:

- **ForwardRequest**  
Specifies whether to forward the discovery request to another active discovery plug-in. The request is forwarded when the current discovery plug-in fails to process the request.
- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 600

**Note:** Applicable only when ScheduleType is set to 2.

- **max\_threads\_count**  
Defines the threadpool threads count.  
**Default:** 10
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 1
- **PluginPath**  
Defines the full pathname of the plugin.  
**Default:** /opt/CA/bin/DiscoveryAgent.dll
- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat  
**Note:** Applicable only when ScheduleType is set to 2.
- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 0

## communication

Privileged Access Manager maintains the message queue server communication settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication
```

The communication registry key contains the following registry entries:

- **certificate**  
Defines the certificate file for the SSL connection.  
**Limits:** The full pathname to a file containing the certificate data.
- **Distribution\_Server**  
Defines the Distribution Server URL. You can define more than one Distribution Server in a comma-separated list.  
**Example:** ssl://ds.comp.com:61616, ssl://ds\_dr.comp.com:61616  
**Default:** none
- **endpoint\_to\_server\_queue**  
Defines the name of the message queue that the endpoint uses to send information to Privileged Access Manager Enterprise Management.  
**Default:** ac\_endpoint\_to\_server
- **ServerVersion**  
Specifies the version of the Distribution Server. Consider that an endpoint is configured to work with a Distribution Server with build version lower than the endpoint. You can set the build version manually and provide the build version of the Distribution Server.  
**Example:** 12.01.0648  
The token is used for forward compatibility functionality in modules like policyfetcher, ReportAgent, Shared Account Management and UNAB.
- **server\_to\_endpoint\_broadcast\_queue**  
Defines the name of the message queue that Privileged Access Manager Enterprise Management uses to broadcast messages to all endpoints.  
**Default:** ac\_server\_to\_endpoint\_broadcast
- **server\_to\_endpoint\_queue**



Defines the name of the message queue that Privileged Access Manager Enterprise Management uses to send messages to the endpoint.

**Default:** ac\_server\_to\_endpoint

- **server\_to\_server\_broadcast\_queue**

Defines the name of the message queue that the Enterprise Management Server uses to broadcast topics and authenticates using the reportserver user.

**Default:** ac\_server\_to\_server\_broadcast

- **server\_to\_server\_local\_queue**

Defines the name of the queue on the Privileged Access Manager Message Queue used by the Distribution Server to get information from the Enterprise Server.

**Default:** ac\_server\_to\_server\_local

- **server\_to\_server\_queue**

Defines the name of the message queue that the Enterprise Management Server uses to send messages and authenticate using the reportserver user.

**Default:** ac\_server\_to\_server

- **ssl\_keystore**

Defines the keystore location and the location of the client certificate for the SSL.

**Limits:** The full pathname to the keystore location.

**Default:** none

- **ssl\_keystore\_pw**

**Default:** none

- **ssl\_noverifyhost**

Specifies whether to enable verification of the host certificate.

**Limits:** 0, disable host certificate verification; 1, enable host certificate verification

**Default:** 0

- **ssl\_noverifyhostname**

Specifies whether to enable verification of the host name.

**Limits:** 0, disable host name verification; 1, enable host name verification

**Default:** 0

- **ssl\_truststore**

Defines the truststore for server verification.

**Limits:** The full pathname to the truststore.

**Default:** none

- **ssl\_truststore\_pw**

**Default:** none

## crypto (Windows)

Privileged Access Manager maintains cryptography module settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\crypto
```

The crypto registry key contains the following registry entries:

- **ca\_certificate**

Defines the full pathname to the Certificate Authority (CA) certificate database.

**Default:** ACInstallDir\data\crypto\def\_root.pem

- **cleanup\_schedule**

Specifies the interval to execute the cleanup task.

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat (Running every day at midnight)

- **communication\_mode**

Specifies whether secure socket layer (SSL) protocols are enabled.

If you set this value to `ssl_only`, only SSL V2, SSL V3, and TLS connections are enabled. This means that this computer cannot communicate with computers that do not support SSL. This computer also cannot communicate with computers that are running versions of Privileged Access Manager earlier than r12.0, which do not support SSL.

#### NOTE

Computers that are running Privileged Access Manager r12.0 and later do support SSL.

If the `fips_only` token is set to 1, the actual communication mode is set to `ssl_only` in FIPS mode (that is, TLS). The `communication_mode` token is ignored.

Valid values are:

- `all_modes`
- `ssl_only`
- `non_ssl`

**Default:** `non_ssl`

- **encryption\_methods**

Specifies the encryption libraries that the Privileged Access Manager Agent uses to decrypt messages. The Agent attempts to use each library in the list, in turn, until the decryption is successful.

**Limits:** `aes256enc`, `aes192enc`, `aes128enc`, `desenc`, `tripledesenc`, `defenc`

**Default:** `aes256enc`, `aes192enc`, `aes128enc`, `desenc`, `tripledesenc`

- **fips\_only**

This token controls whether Privileged Access Manager works in FIPS only mode. In this mode, all non-FIPS functions are disabled.

Valid values:

**1** Privileged Access Manager works in FIPS only mode

**0** Privileged Access Manager works in non-FIPS mode

**Default:** 0

- **private\_key**

Defines the full pathname to the subject private key.

**Default:** `ACInstallDir\data\crypto\sub.key`

- **refresh\_timeout**

Specifies the interval to refresh an internal cache and resolve the IP address of the connected host.

**Default:** 86400 seconds (24 hours)

- **sha\_mode**

Defines the hashing mode for SHA signatures.

**Values:** `sha1`, `sha256`, `sha384`, `sha512`

**Default:** `sha512`

- **ssl\_hostname\_validation**

Specifies whether the certificate hostname validation is enabled during a secure connection.

**Default:** 0

#### NOTE

The certificate hostname validation is not performed during a secure connection.

- **ssl\_port**

Defines the port for SSL communications between Privileged Access Manager clients and services.

**Default:** 5249

- **subject\_certificate**

Defines the full pathname to the subject certificate.

**Default:** `ACInstallDir\data\crypto\sub.pem`

## Data

Privileged Access Manager maintains internal settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Data
```

Data key entries are for internal use only. You cannot open this key.

## Dependency (Registry Settings)

Privileged Access Manager maintains dependency settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Dependency
```

When the Privileged Access Manager component module is installed as an embedded component of another product, all subkeys of this registry key are the name of the product that is dependent on Privileged Access Manager. If you upgrade or uninstall Privileged Access Manager, it checks this registry and decides whether the process can continue or if it must be aborted.

## devcalc (Windows)

Privileged Access Manager maintains deviation calculator settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\devcalc
```

The devcalc registry key contains the following registry entries:

- **dms\_cmd\_retry\_interval**  
Defines the number of seconds between each DMS notification command retry.  
**Default:** 60
- **max\_dms\_cmd\_retry**  
Defines the maximum number of times the policy deviation calculator retries to send update notifications to the DMS before stopping.  
**Default:** 3
- **max\_lines\_request**  
Defines the maximum number of lines (from the policy deviation data file) that the *get devcalc* selang command returns at any one time. You then retrieve more lines using the following command:

```
get devcalc params("offset=X")
```

X Defines the line offset returned by the previous *get devcalc* output.

```
get devcalc params("offset=X")
```

– X

Defines the line offset returned by the previous *get devcalc* output.

**Default:** 50

## Exits

Privileged Access Manager maintains agent exit settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits
```

The Exits registry key does not contain any registry entries. It contains registry subkeys for every agent exit.

## AuthenticatePassword

Privileged Access Manager maintains password authentication agent exit settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\AuthenticatePassword
```

The Exits\AuthenticatePassword registry key contains the following registry entries:

- **Enable**  
The toggle to enable or disable the password rules enforcement agent exit. A value of 0 disables the exit. Any other value enables it.  
**Default: 0**
- **EnforcePasswordControl**  
The conditions for password rules enforcement using a Privileged Access Manager client:  
0 - no password rules enforcement  
1 - password rules enforcement is activated when regular users change their own passwords  
2 - password rules enforcement is activated when an admin or a password manager changes someone else's or their own password  
3 - accumulation of values 1 and 2  
**Default: 1**

## Engine

Privileged Access Manager maintains the engine (seos) agent exit settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Engine
```

The Exits\Engine registry key does not contain any registry entries by default.

## Remote Grace Info

Privileged Access Manager maintains remote grace information agent exit settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Grace Info
```

The Exits\Remote Grace Info registry key contains the following registry entry:

- **DefaultWarningDays**  
Defines the default number of days for a password expiration warning display to users of segrace\SegraceW utilities. It means that if one of these utilities is being applied and the password of the user is to expire in fewer days than specified by this registry value, then a warning message for the user is displayed.  
**Default: 7**

## Remote Shutdown

Privileged Access Manager maintains remote shutdown agent exit settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Shutdown
```

The Exits\Remote Shutdown registry key contains the following registry entries:

- **Path**  
The full path name of the remote shutdown DLL.  
**Default: AC\InstallDir\bin\remshut.dll**
- **Prefix**  
The defined prefix used by the remote shutdown DLL.  
**Default: SD**

## Script Engine

Privileged Access Manager maintains the script engine settings that it uses under the following key:

```
HKEY_CURRENT_USER\Software\ComputerAssociates\AccessControl\ScriptEngine
```

The script Engine registry key contains the following registry entries:

### Locale

**Type:** REG\_DWORD

**Values:** 0x409

#### NOTE

The Current user locale default value is English.

### PuttyLocation

**Type:** REG\_SZ

#### NOTE

ActiveX sets this value during the first SSH autologin attempt.

### TraceEnabled

**Type:** REG\_DWORD

**Values:** 1

#### NOTE

Trace messages are sent to the windows debugger or dbgview.exe for display.

## Sessions

Privileged Access Manager maintains the script engine sessions settings that it uses under the following key:

```
HKEY_CURRENT_USER\Software\ComputerAssociates\AccessControl\ScriptEngine\sessions
```

The sessions registry key contains the following registry entries:

**<user@hostname>**

**Type:** REG\_DWORD

#### NOTE

ActiveX maintains a counter of the number of open sessions to show the last closing session check-in dialog.

## FsiDrv

Privileged Access Manager maintains driver settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\FsiDrv
```

The FsiDrv registry key contains the following registry entries:

- **AuditRefreshPeriod**  
Defines the minimum time in seconds between two consecutive audit events from the same source. Privileged Access Manager does not log audit messages for consecutive events from the same source that occur within this time period.  
**Default:** 0 (all audit events are logged)
- **BatchOplockStatus**  
Specifies whether to disable batch OpLocks (opportunistic locking) of an entire file. When disabled (value is zero), the driver collects 100 percent of audit information for file access but performance decreases. A non-zero value keeps

batch OpLocks operating regularly (enabled) and increases performance, but potentially provides incomplete audit information that may not include attempts to access related files.

**NOTE**

You must reload the driver to use the new setting. Unload the driver (net stop seosdrv) after you stop Privileged Access Manager (secons -s).

**Default:** 1 (enabled)

- **BypassDriversCount**

Defines how many drivers you want to add to your bypass list.

**Type:** REG\_DWORD

**Default:** 0

- **CacheLimit**

Defines the seosdrv kernel memory cache limit size in megabytes.

**Type:** REG\_DWORD

**Limits:** 8 - 64

**Default:** 16

- **CounterResolution**

Defines the time stamp measurement resolution using the following format: a:1000.

**Type:** DWORD

**Limits:** 1 - 1000 (decimal)

**Default:** 100

- **DefLookupThreads**

Defines the number of threads that Privileged Access Manager opens to resolve SIDs into account names.

**Default:** 5

- **directory**

The location of the driver.

**Default:** *system\_drive\Windows\_path\system32\drivers*

- **DriverName\_drvNumber**

Defines the name of a driver that you want to bypass. Example: thisdrv.sys.

**Values:** drvNumber - a number from 0 to BypassDriversCount - 1.

**Type:** REG\_SZ

**Limit:** 49 characters.

**NOTE**

Create one registry entry for each driver that you want to bypass and verify that the BypassDriversCount specifies the number of drivers you defined.

- **DynamicSysThreadDetection**

Specifies that Privileged Access Manager traces all kernel mode threads that are created by another product which creates system threads. Example: Trend Micro PC-cillin Antivirus.

**NOTE**

Enabling this registry value can cause performance issues. We recommend that you contact Broadcom Support before you enable this registry value. For assistance, contact Broadcom Support at <https://www.broadcom.com/support>.

**Type:** REG\_DWORD

**Default:** 0 (disabled)

- **FileCacheDisabled**

The toggle to enable or disable the generic file cache.

**Values:** 0enable the generic file cache, 1disable the generic file cache

**Default:** 0

- **LoopHoleProtectionDisabled**

Specifies whether to disable loophole protection, which protects Privileged Access Manager from applications such as Process Monitor (procmon.exe) that can close its handles.

**Values:** **0** - enable loophole protection; **1** - disable loophole protection.

**Default:** 0

- **MaxAuditRecordLimit**

Defines the audit queue limit. When the queue length exceeds this limit, Privileged Access Manager artificially slows down threads that generate audit events. In this way, it can read the queue and can write to the log file faster than new items are added to the queue.

**NOTE**

When new items are added to the queue faster than Privileged Access Manager can read and process them, the system's memory may be exhausted.

**Default:** 200

- **MaxTimeoutLimit**

Defines the number of consecutive timeouts that Privileged Access Manager detects before it triggers a driver bypass. Once reached, the driver stops sending authorization requests to the authorization engine until the engine indicates that it is ready to process events.

A value of zero disables this bypass.

**Default:** 5

- **QueueTimeout**

The maximum time in seconds to wait for seosd to respond.

**Default:** 10

- **QueueTimeoutAnswer**

The response of the driver after time-out.

**Default:** 0 (Deny)

- **RedRangeLimit**

Defines the range of accumulated authorization timeout in comparison to the queue timeout.

**Type:** DWORD

**Values:** 70 - 99

**Default:** 70

- **RegistryCacheDisabled**

The toggle to enable or disable the generic registry cache.

**Values:** 0 enable the generic registry cache, 1 disable the generic registry cache

**Default:** 0

- **SilentModeAdmins**

- Line separated list of user names who can administer the computer in maintenance mode (SilentModeEnabled = 1).  
No default

- **SilentModeEnabled**

Determines whether maintenance mode is active (1).

**Default:** 0 (disabled)

- **SystemBypassRestricted**

Specifies if Privileged Access Manager bypasses access checks for system processes. By default, Privileged Access Manager does not consider system processes to be trusted and does not bypass access checks for system processes.

**Values:** **0** - bypass access checks; **1** - do not bypass access checks.

**Default:** 1

- **YellowRangeLimit**

Defines the range of accumulated authorization timeout in comparison to the queue timeout value. For example, if the driver authorization queue contains 15 events and the average processing period is 0.1 seconds, then the accumulated authorization timeout is 1.5 seconds, which represents 15% of 10 seconds. The value below the yellow range sets the state to green. The value above the yellow range sets the state to red.

**Type:** DWORD

**Values:** 20 - 50

**Default:** 40

## Instrumentation

Privileged Access Manager maintains cainstrm.dll behavior settings (which apply to all loaded plug-ins) it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation
```

The Instrumentation registry key contains the following registry entries:

- **Active**  
Specifies whether cainstrm.dll is active (1).  
If you specify 0, cainstrm.dll loads but does not process any plug-ins.  
**Type:** REG\_DWORD  
**Default:** 1
- **ApplyOnProcess**  
Specifies a list of processes on which cainstrm.dll is loaded/applied.  
If the list is empty then cainstrm.dll is applied on all processes not listed in ExcludeProcess.  
If the list is not empty then cainstrm.dll is applied on the listed processes only and ignores processes listed in ExcludeProcess.  
You can define the name of the service or the full pathname. Names are *not* case sensitive. For example, "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".  
**Type:** REG\_MULTI\_SZ  
By default, this token is not set (instrumentation applies to any process).
- **ExcludeProcess**  
Specifies a list of processes to which instrumentation does *not* apply.  
  
**NOTE**  
This entry is valid only if ApplyOnProcess is not set.  
**Type:** REG\_MULTI\_SZ  
By default, this token is not set.
- **OperationMode**  
Specifies whether cainstrm.dll loads plug-ins (1) or not (0).  
**Type:** REG\_DWORD  
**Default:** 1
- **RunTimeInstrumentationDisabled**  
Specifies the Privileged Access Manager instrumentation policy at run time.  
**Type:** REG\_DWORD  
**Limits:** 0 - runtime instrumentation enabled; 1 - runtime instrumentation disabled  
**Default:** 0
- **RunTimeInstrumentationIncludeList**  
Specifies a list of processes to apply the runtime instrumentation to.  
**Type:** REG\_MULTI\_SZ
- **TraceDbgEnable**  
Specifies whether to trace status flag for the cainstrm module. The key entry enables tracing into DbgView or Kernel Debugger.  
**Type:** REG\_DWORD  
**Limits:** 0 - false; 1 - true  
**Default:** 0
- **TraceFileIsCyclic**  
Specifies the type of the trace file.



**Type:** REG\_DWORD

**Limits:** 0 - trace file is not cyclic; 1 - trace file is cyclic

**Default:** 0

- **TraceFileSizeLimit**

Defines the maximum size of the trace file in bytes. A value of 0 means no maximum size limit is imposed on the trace file.

**Type:** REG\_DWORD

**Default:** 0

- **TraceFilteringMask**

Defines the filtering mask for each plug-in. The supported values for this registry value change depending on the status of the software component for which you define the registry value. Two values are predefined: 0, all information is filtered (display no information); 0x0fffffff, no information is filtered (display all information).

**Type:** REG\_DWORD

**Default:** 0

**NOTE**

We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at <http://ca.com/support>.

- **TraceFolderPath**

Defines the full pathname to the trace file.

**Type:** REG\_SZ

- **TraceOutputMask**

Defines the filtering mask for the trace output channels - debug stream, file, or ETW. You can specify that the trace outputs to file, to DbgView debug channel, or to WinDbg debug channel. A value of 0 disables any output.

**Type:** REG\_DWORD

**Default:** 0

**NOTE**

We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at <http://ca.com/support>.

- **UnloadIfNoPlugins**

Specifies whether cainstrm.dll is automatically unloaded (1) when no plug-ins are assigned to a current process. If you specify 0, cainstrm.dll loads but does not process plug-ins.

**Type:** REG\_DWORD

**Default:** 1

## **\_Dot NET**

Privileged Access Manager maintains .NET instrumentation under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\.NET
```

The .NET registry key contains the subkey - Profiler.

Described below are the registry entries in the Profiler subkey:

- **ApplyOnProcess** Defines a list of processes to load the .NET Profiler.

**Type:** REG\_MULTI\_SZ

- **CLSID** Specifies a globally unique identifier that identifies an object.

For internal use. Not changeable.

**Type:** REG\_SZ

- **OperationMode** Defines whether to load the .NET Profiler into the memory.

**Limits:** 0 - False; 1 - True

**Type:** REG\_DWORD

- **ReadConfigPeriodSec** Defines interval (in seconds) for the plugin to read its configuration from the Registry.  
**Type:** REG\_DWORD
- **TraceDbgEnable**  
Specifies whether to trace status flag for the cainstrm module. The key entry enables tracing into DbgView or Kernel Debugger.  
**Type:** REG\_DWORD  
**Limits:** 0 - False; 1 - True  
**Default:** 0
- **TraceFileEnable** Enables tracing into the file.  
**Type:** REG\_DWORD  
**Default:** 0 - disabled
- **TraceFileIsCyclic** Specifies the type of the trace file.  
**Type:** REG\_DWORD  
**Limits:** 0 - trace file is not cyclic; 1 - trace file is cyclic  
**Default:** 0
- **TraceFileSizeLimit** Defines the maximum size of the trace file in bytes. A value of 0 means no maximum size limit is imposed on the trace file.  
**Type:** REG\_DWORD  
**Default:** 0
- **TraceFilteringMask** Defines the filtering mask for each plug-in. The supported values for this registry value change depending on the status of the software component for which you define the registry value.  
**Limits:** 0 - all information is filtered (display no information); 0x0fffffff - no information is filtered (display all information).  
**Type:** REG\_DWORD  
**Default:** 0

#### NOTE

We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at <http://ca.com/support>.

- **TraceFolderPath** Defines the full pathname to the trace file.  
**Type:** REG\_SZ
- **TraceOutputMask**  
Defines the filtering mask for the trace output channels - debug stream, file, or ETW. You can specify that the trace outputs to file, to DbgView debug channel, or to WinDbg debug channel. A value of 0 disables any output.  
**Type:** REG\_DWORD  
**Default:** 0

#### NOTE

We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at <http://ca.com/support>.

- **TraceReadParamsSec** Specifies the time taken to read the trace parameters from the registry.  
**Type:** REG\_DWORD  
**Default:** 60 seconds

The Profile sub key contains the following subkeys with registry entries for internal use only and are not changeable:

- Assemblies
- Plugins

## Plugins

Privileged Access Manager maintains settings that are used by the plugins under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
```

The Plugins key does not contain any registry entries. It contains registry subkeys for plugins.

### **AccountManager**

Privileged Access Manager maintains the Account Manager related settings in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager\Plugins
\AccountManager
```

The Account Manager registry key contains the following registry entries:

- **ComponentName**  
Specifies the name of the AgentManager plug-in.
- **Exclude\_Endpoint\_Types**  
Defines the endpoints types that the current AccountManager does not process.  
**Values:** A comma separated list of endpoint types.  
**Example:**  
  

```
exclude_endpoint_types = Windows Agentless
```
- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 1  
**Note:** Applicable only when ScheduleType is set to 2.
- **JCS\_add\_timeout**  
Specifies JCS timeout in seconds during an *add* operation.  
**Default:** 300
- **JCS\_modify\_timeout** Specifies JCS timeout in seconds during a *modify* operation.  
**Default:** 300
- **JCS\_search\_timeout** Specifies JCS timeout in seconds during a *search* operation.  
**Default:** 300
- **max\_threads\_count**  
Defines the number of working threads in the pool.  
**Values:** 50  
**Type:** REG\_DWORD
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 0
- **PluginPath**  
Defines the full pathname of the plugin.  
**Type:** REG\_SZ  
**Default:** \ProgramFiles\CA\PAMSCServer\APMS\PAMSC\bin\AccountManager.dll
- **QueryFilter**  
Specifies additional values that are added to the Message Queue receive queue filter.  
**Options:** ENDPOINT\_CUSTOM 1...5=, ENDPOINT\_OWNER=, ENDPOINT\_DEPARTMENT=

**NOTE**

- Place property values in apostrophes
- Use AND and OR operands to specify more than a single property
- Use parenthesis when needed
- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

**NOTE**

Applicable only when ScheduleType is set to 2.

- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 1
- **wmi\_timeout**  
Defines in seconds how long WMI waits for a response from the endpoint before timeout.  
**Default:** 60

**PupmAgentManager**

Privileged Access Manager maintains the PupmAgentManager related settings in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
\PupmAgent
```

The PupmAgentManager registry key contains the following registry entries:

- **AutoRegister**  
Defines the auto registration interval in days.  
**Default:** 7
- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 1  
**Note:** Applicable only when ScheduleType is set to 2.
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 0
- **PluginPath**  
Defines the full pathname of the plugin.  
**Default:** /opt/CA/PAMSCShared/lib/AccountManager.so
- **RegistrationInterval**  
Specifies the registration schedule in intervals.  
**Default:** 7  
**Type:** REG\_DWORD
- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

**NOTE**

Applicable only when ScheduleType is set to 2.

- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 1

**DiscoveryAgent**

Privileged Access Manager maintains settings that are related to the DiscoveryAgent in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
\DiscoveryAgent
```

The DiscoveryAgent registry key contains the following registry entries:

- **ForwardRequest**  
Specifies whether to forward the discovery request to another active discovery plug-in. The request is forwarded when the current discovery plug-in fails to process the request.
- **Interval**  
Defines the plugin schedule in seconds.  
**Default:** 600  
**Note:** Applicable only when ScheduleType is set to 2.
- **max\_threads\_count**  
Defines the threadpool threads count.  
**Default:** 10
- **OperationMode**  
Defines the plugin operation mode.  
**Options:** 0 - plugin disabled, 1 - plugin enabled  
**Default:** 1
- **PluginPath**  
Defines the full pathname of the plugin.  
**Default:** /opt/CA/bin/DiscoveryAgent.dll
- **Schedule**  
Defines the plugin scheduling string.  
**Default:** 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat  
**Note:** Applicable only when ScheduleType is set to 2.
- **ScheduleType**  
Defines the plugin schedule type.  
**Options:** 0 - execute once, 1 - execute on demand, 2 - execute on interval, 3 - execute on schedule  
**Default:** 0

**PluginManagement**

Privileged Access Manager maintains internal plugin management under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PluginManagement
```

The PluginManagement key contains the following registry entries:

- **Active**  
Internal use only and not changeable.

Specifies whether cainstrm.dll is active (1).

**Type:** REG\_DWORD

**Default:** 1

- **Altitude** Internal use only and not changeable.  
Defines the order to load the plug-in.  
**Type:** REG\_DWORD
- **ApplyOnDLL** Internal use only and not changeable.  
Defines the DLL names (modules) to load the plug-in.  
**Type:** REG\_MULTI\_SZ
- **ApplyOnProcess** Internal use only and not changeable.  
Specifies a list of processes on which cainstrm.dll is loaded/applied.  
If the list is empty then cainstrm.dll is applied on all processes not listed in ExcludeProcess.  
If the list is not empty then cainstrm.dll is applied on the listed processes only and ignores processes listed in ExcludeProcess.  
**Type:** REG\_MULTI\_SZ  
By default, this token is not set (instrumentation applies to any process).
- **ExcludeProcess** Internal use only and not changeable.  
Specifies a list of processes to which instrumentation does *not* apply.

#### NOTE

This entry is valid only if ApplyOnProcess is not set.

**Type:** REG\_MULTI\_SZ

By default, this token is not set.

- **LoadLibraryA** Internal use only and not changeable.  
**Type:** REG\_DWORD
- **LoadLibraryExA** Internal use only and not changeable.  
**Type:** REG\_DWORD
- **LoadLibraryExW** Internal use only and not changeable.  
**Type:** REG\_DWORD
- **LoadLibraryW** Internal use only and not changeable.  
**Type:** REG\_DWORD
- **OperationMode** Internal use only and not changeable.  
Specifies whether cainstrm.dll loads plug-ins (1) or not (0).  
**Type:** REG\_DWORD  
**Default:** 1
- **PluginName** Internal use only and not changeable.  
Defines the name of the Dynamic Link Library (DLL) for the plug-in.  
**Type:** REG\_SZ
- **ProcessCommandArguments** Internal use only and not changeable.  
**Type:** REG\_DWORD

#### NOTE

The PluginManagement registry entries are for internal use only. Do not change their value.

## lang Registry

Privileged Access Manager maintains management language (selang) settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang
```

The lang registry key contains the following registry entries:

- **HandleHomeDir**

The value that determines whether property HOME\_DIR for native user account is updated and home directory created.

If the value is set to 0, only user's property HOME\_DIR is updated. If the value is set to 1, user's property is updated and home directory is physically created in the file system.

**Default:** 1

- **help\_path**

The directory in which the lang help files are located.

**Default:** *ACInstallDir\data\help*

- **HNODE\_MAX\_EVENTS**

Defines the maximum number of health status events being written to the HNODE record. If the number of events exceeds the maximum, the product removes the oldest events and leaves the newest events only.

**Default:** 10

- **ModifiableClassFlags**

Specifies the flags that an Privileged Access Manager administrator can change using the following selang command: `setoptions class className flags{+ | -} (flag)`

**Values:** W - Set Warning mode for the specified class; I - Change case sensitivity for resources in the specified class; WI - Set Warning mode and change case sensitivity for resources in the specified class

**Default:** W

- **query\_size**

The maximum number of records to be listed in a database query.

**Default:** 100

- **SetBlockRun**

Specifies whether to check if a program is trusted and block the execution of untrusted programs.

**Values:**

**yes**-All programs defined with viapgm authorization rules have the blockrun property set to yes.

**no**-All programs defined with viapgm authorization rules have the blockrun property set to no.

**Default:** Yes

- **SpaceReplace**

For internal use only. This key should always be empty.

**Default:** ""

- **use\_old\_commands**

Specifies whether to disable old ACF2 compatibility commands (ag, lg, rg, lu, au, and so on).

**Limits:** 0 - do not support old commands, 1 - support old commands

**Default:** 1 (support old commands)

## logmgr Registry

Privileged Access Manager maintains logging settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\logmgr
```

The logmgr registry key contains the following registry entries:

- **audit\_back**

The name of the Privileged Access Manager audit backup file. Only Privileged Access Manager can write to this file.

**Default:** *ACInstallDir\log\seos.audit.bak*

- **audit\_group**

The group that can read the audit logs.

**Default:** ComputerAssociates

- **audit\_log**

The name of the Privileged Access Manager audit log file. When this file reaches the size that is specified in `audit_size`, Privileged Access Manager closes the file, renames it with the name in `audit_back`, and creates an audit log. Only Privileged Access Manager can write to this file.

**Default:** *AC\InstallDir\log\seos.audit*

- **audit\_max\_files**

Defines the maximal number of audit log backup files Privileged Access Manager accumulates when it performs date-triggered backups. When the *BackUp\_Date* configuration setting is set to anything other than *none*, Privileged Access Manager continuously accumulates date-triggered backup files. This configuration setting lets you reduce disk space Privileged Access Manager uses for audit log backups. When the number of audit log backup files reaches the limit that you set, Privileged Access Manager deletes the oldest backup file when it creates the newest.

**Values:**

**0** - keep all audit log backup files.

***n*** - a positive integer greater than zero.

**Note:** You cannot remove redundant audit log backup files manually because Privileged Access Manager protects these files automatically. Also, if the audit reporting is enabled, Privileged Access Manager does not delete a backup file until the Report Agent finishes processing it.

**Default:** 50

- **audit\_size**

The maximum size, in KB, of the Privileged Access Manager audit log file. Do not specify less than 50 KB.

**Default:** 10240

**NOTE**

Privileged Access Manager stops writing audit records to the audit file when the audit file size exceeds 2 GB.

- **AuditFiltersFile**

The name of the Privileged Access Manager audit filter file.

**Default:** *AC\InstallDir\data\audit.cfg*

- **BackUp\_Date**

Specifies the criterion by which Privileged Access Manager backs up the audit log file, and if Privileged Access Manager adds a timestamp to the backup file name.

Privileged Access Manager *always* backs up the audit log file when it reaches the size specified in the *audit\_size* configuration setting.

**Values:** none, yes, daily, weekly, monthly

- **yes** - Privileged Access Manager backs up the audit log file when it reaches the size specified in *audit\_size* and adds a timestamp to the backup file name.

- **none** - Privileged Access Manager backs up the audit log file when it reaches the size specified in *audit\_size* and does not add a timestamp to the backup file name.

- **daily, weekly, monthly** - Privileged Access Manager backs up the audit log file whenever the specified interval has elapsed *and* when it reaches the size specified in *audit\_size*, and adds a timestamp to the backup file name. However, if no audit events are written to the audit log file in the specified interval, Privileged Access Manager does not back up the file after the interval elapses.

**Note:** Privileged Access Manager counts the specified interval from the time that it creates the first audit log file, and backs up the file at midnight on the appropriate day.

**Example:** The configuration setting has a value of *weekly* and Privileged Access Manager creates the audit log file at 9:00 am on Friday April 1. Many audit events occur this week and the audit log file exceeds the *audit\_size* configuration setting on Monday 4 April. Privileged Access Manager backs up the audit log file on 4 April and adds a timestamp to the backup file name. A week after the audit log file was first created, at midnight Friday 8 April, Privileged Access Manager again backs up the audit log file and adds a timestamp to the backup file name.

**Limits:** Specify values in all uppercase or all lowercase.

**Default:** none

- **error\_back**

The name of the Privileged Access Manager error backup file.

**Default:** *AC\InstallDir\log\seos.error.bak*

- **error\_group**

The group that can read the error log files.

If this value is set to *none*, only Administrators can read the file.



**Default:** none

- **error\_log**  
The name of the Privileged Access Manager error log file. When this file reaches the size specified in `error_size`, Privileged Access Manager closes the file, renames it with the name in `error_back`, and creates an error log. Only Privileged Access Manager can write to this file.  
**Default:** *ACInstallDir\log\seos.error*
- **error\_size**  
The maximum size, in KB, of the Privileged Access Manager error log file.  
**Default:** 50
- **irecorder\_audit**  
Specifies whether the IR API library routes audit events of existing PMDs in addition to the local security service audit events.  
**all** - routes audit events of Policy Models in addition to the local security service audit events.  
**localhost** - routes audit events of the local security service only.  
**Default:** all
- **SendAuditToNativeChannel**  
(Windows 2008 only) Specifies whether seosd sends audit events to the Windows 2008 event log channel for Privileged Access Manager.  
**Default:** 0 (no)
- **SendAuditToNativeLog**  
Specifies whether seosd sends audit events to the Windows event log.  
**Default:** 0 (no)

## message Registry

Privileged Access Manager maintains messaging settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\message
```

The message registry key contains the following registry entries:

- **filename**  
The name of the file that supplies most of the messages that appear in response to Privileged Access Manager commands.  
**Default:** *ACInstallDir\Data\SeOS.msg*
- **MessagesDirectory**  
Specifies the location of the Privileged Access Manager messages file.  
**Default:** *ACInstallDir\Data\Messages*

## OS\_User

Privileged Access Manager maintains enterprise user settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\OS_user
```

The OS\_user registry key contains the following registry entries:

- **create\_user\_in\_db**  
Specifies whether Privileged Access Manager creates an XUSER record for an undefined user, when that user logs in.  
**Note:** This setting applies only if you use enterprise users (`osuser_enabled` is set to 1).  
Following are the valid values:  
**0** - Privileged Access Manager does not automatically create an XUSER record.  
**1** - Privileged Access Manager automatically creates an XUSER record

**Default:** 1

- **osuser\_enabled**

Specifies whether enterprise users and groups are enabled.

Following are the valid values:

**0** - The use of enterprise users and groups is disabled.

**1** - The use of enterprise users and groups is enabled.

**Default:** 1

## passwd Registry

Privileged Access Manager maintains password settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd
```

The passwd registry key contains the following registry entries:

- **DefaultPgroup**

Internal use only

**Default:** other

- **Dictionary**

Defines the full pathname of the file containing the words that *cannot* be used as passwords.

**NOTE**

To use this file, set the dictionary format password rule (use\_dbdict) to *file* and set UseDict setting to *yes*.

If the dictionary format is set to *db*, passwords that cannot be used are taken from the Privileged Access Manager database and this setting is ignored.

**Default:** *ACInstallDir\data\words*

- **EnforceViaEtrust**

Specifies whether to enforce updating or creating user passwords through Privileged Access Manager only.

**Default:** 0 (do not have to use Privileged Access Manager)

- **NativePasswordPropagation**

Specifies that a Password filter propagates passwords in Privileged Access Manager and native environments.

**Default:** 1

If 0 is set, the password propagation is done into the Privileged Access Manager environment only. If 1 is set, the Password filter propagates passwords into Privileged Access Manager and native environments.

- **PasswordTimeout**

Defines the maximum number of milliseconds that the Privileged Access Manager password filter waits for authorization response.

**Default:** 4000

- **PasswordTimeoutAnswer**

Specifies the answer to send back to the LSA if the authorization process does not respond in the time-out given.

If 0 is set, the password change is refused. If 1 is set, the password change is approved.

**Default:** 0

- **UseDict**

Specifies whether to use the dictionary file (set with the Dictionary setting) when verifying a password.

**NOTE**

To use the dictionary file, you must also set the dictionary format password rule (use\_dbdict) to *file*. If the dictionary format is set to *db*, passwords that cannot be used are taken from the Privileged Access Manager database and this setting is ignored.

**Default:** no

## pmd

Privileged Access Manager maintains generic Policy Model settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd
```

The Pmd registry key contains the following registry entries:

- **\_\_pmd\_backup\_directory\_\_**  
Defines the directory that Privileged Access Manager uses to store Policy Model backups. Privileged Access Manager stores each PMD backup in a subdirectory named *pmd\_name*.  
**Default:** *ACInstallDir\Data\policies\_backup*
- **\_Pmd\_directory\_**  
Defines the directory in which PMDB database files are located.  
**Default:** *ACInstallDir\Data*
- **ClientOperationTimeout**  
Defines the number of seconds a Policy Model client on this computer waits for a response from the Policy Model. If the Policy Model does not respond within this time frame, the Policy Model client assumes that the Policy Model is nonresponsive.  
**Default:** 60
- **MaximumPolicyModels**  
Defines the maximum number of policy models you can create.  
**Default:** 16
- **SendAuditToNativeChannel**  
(Windows 2008 only) Specifies whether PMDB sends audit events to the Windows 2008 event log channel for Privileged Access Manager.  
**Default:** 0
- **SendAuditToNativeLog**  
Specifies if Privileged Access Manager sends Policy Model audit events to the Windows event log.  
**Values:** 0 - do not send audit events to the Windows event log, 1 - send audit events to the Windows event log  
**Default:** 0
- **ShutdownWaitingTimeout**  
Defines the number of milliseconds a Policy Model on this computer waits for its components to shut down gracefully. If Policy Model components do not shut down gracefully within this time frame, the Policy Model forces them to shut down.  
**Default:** 60000 (1 minute)
- **TCPReceiveTimeout**  
Defines the number of seconds a Policy Model on this computer waits for a response from its subscribers. If a Policy Model subscriber does not respond within this time frame, the Policy Model closes its connection to it.  
**Default:** 60

## <PMDB\_Name>

Privileged Access Manager maintains specific Policy Model settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\PMDB_Name
```

Each Pmd\PMDB\_Name registry key contains the following registry entries:

- **\_Min\_Retries**  
Defines the number of failed attempts the Policy Model makes to connect to a subscriber before it considers it unavailable.  
**Default:** 4
- **\_Retry\_Timeout**

Defines the time, in minutes, that the Policy Model waits before trying to resend an update to an unavailable subscriber, after the minimum number of attempts specified in `_Min_Retries` has been made.

**Default:** 30

- **\_Shutoff\_Time\_**  
Obsolete.
- **Active\_Policy**  
Defines the Policy Model name.
- **Always\_Propagate**  
Specifies whether the Policy Model propagates commands when there is an error. By default, the Policy Model always sends commands for propagation. If you set this to *no* the Policy Model will not send command when there is an error.  
**Default:** Yes
- **Auto\_Truncate**  
Specifies if `sepm` truncates the updates file if you execute `sepm -t` without specifying either `auto` or the offset.  
**Values:** Yes `sepm` automatically truncates the update file if no `sepm -t` parameter is specified, No `sepm` does not truncate the update file if no `sepm -t` parameter is specified  
**Default:** Yes
- **Filter**  
Defines the full pathname of the filter file for the update file.  
No default.
- **force\_auto\_truncate**  
Specifies whether Privileged Access Manager truncates the update file even if there are no subscribers to the Policy Model.  
You can truncate the update file manually (`sepm -t`), and Privileged Access Manager also truncates the file automatically based on a separate configuration setting (`trigger_auto_truncate`) that defines the event that triggers automatic truncation.  
**Note:** If all subscribers to the Policy Model are "Out of sync", the Policy Model effectively has no subscribers.  
**Default:** Yes
- **Parent\_Pmd**  
Defines the names of parent PMDBs from which this Policy Model accepts updates.  
No default.
- **trigger\_auto\_truncate**  
Defines the size of the Policy Model update file, in megabytes, that triggers an automatic truncating of the update file. If you set this entry to 0, Privileged Access Manager uses the hard-coded default value (100 MB). If you use a value that is greater than the upper limit, Privileged Access Manager uses the upper limit value.  
**Type:** REG\_DWORD  
**Limits:** 1 - 2000 MB  
**Default (DMS\_\_ and DH\_\_WRITER):** 1024 MB  
**Default (all other PMDBs):** 100 MB
- **UseEncryption**  
Specifies whether update information that is saved to the `updates.dat` file is encrypted.  
**Values:** 0 Do not encrypt the `updates.dat` file, 1 encrypt the `updates.dat` file  
**Default:** 0

## logmgr key

Privileged Access Manager maintains specific Policy Model log settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\PMDB_Name\logmgr
```

Each `Pmd\PMDB_Name\logmgr` registry key contains the following registry entries:

- **audit\_back**  
Defines the name of the Policy Model audit backup file. Only Privileged Access Manager can write to this file.

- Default:** pmd\_audit.bak
- **audit\_group**  
Defines the group that can read the audit logs.  
**Default:** Computer Associates
- **audit\_log**  
Defines the name of the Policy Model audit log file. When this file reaches the size specified in `audit_size`, Privileged Access Manager closes the file, renames it with the name set in `audit_back`, and creates a new audit log.  
Only Privileged Access Manager can write to this file.  
**Default:** pmd.audit
- **audit\_size**  
Defines the maximum size, in KB, of the Policy Model audit log file. Do not specify a value that is less than 50 KB.  
**Default:** 1024
- **error\_back**  
Defines the name of the Policy Model error backup file.  
**Default:** pmd\_error.back
- **error\_group**  
Defines the group that can read the error log files.  
If this value is set to *none*, only Administrators can read the file.  
**Default:** none
- **error\_log**  
Specifies the name of the Policy Model error log file. When this file reaches the size specified in `error_size`, Privileged Access Manager closes the file, renames it with the name in `error_back`, and creates a new error log. Only Privileged Access Manager can write to this file.  
**Default:** pmd.error
- **error\_size**  
Defines the maximum size, in KB, of the Privileged Access Manager error log file.  
**Default:** 1024

## DMS Name

Privileged Access Manager maintains specific DMS settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\DMS_Name
```

The `Pmd\DMS_Name` registry key contains the following registry entries:

- **\_Min\_Retries**  
Defines the number of failed attempts the Policy Model makes to connect to a subscriber before it considers it unavailable.  
**Default:** 4
- **\_Retry\_Timeout**  
Defines the time, in minutes, that the Policy Model waits before trying to resend an update to an unavailable subscriber, after the minimum number of attempts specified in `_Min_Retries` has been made.  
**Default:** 30
- **\_Shutoff\_Time\_**  
Obsolete.
- **Active\_Policy**  
Defines the Policy Model name.
- **Always\_Propagate**  
Specifies whether the Policy Model propagates commands when there is an error. By default, the Policy Model always sends commands for propagation. If you set this to *no* the Policy Model will not send command when there is an error.

**Default:** Yes

- **Auto\_Truncate**  
Specifies if sepmd truncates the updates file if you execute sepmd -t without specifying either auto or the offset.  
**Values:** Yessepmd automatically truncates the update file if no sepmd -t parameter is specified, Nosepmd does not truncate the update file if no sepmd -t parameter is specified  
**Default:** Yes
- **Filter**  
Defines the full pathname of the filter file for the update file.  
No default.
- **force\_auto\_truncate**  
Specifies whether Privileged Access Manager truncates the update file even if there are no subscribers to the Policy Model.  
You can truncate the update file manually (sepmd -t), and Privileged Access Manager also truncates the file automatically based on a separate configuration setting (trigger\_auto\_truncate) that defines the event that triggers automatic truncation.  
**Note:** If all subscribers to the Policy Model are "Out of sync", the Policy Model effectively has no subscribers.  
**Default:** Yes
- **Parent\_Pmd**  
Defines the names of parent PMDBs from which this Policy Model accepts updates.  
No default.
- **trigger\_auto\_truncate**  
Defines the size of the Policy Model update file, in megabytes, that triggers an automatic truncating of the update file. If you set this entry to 0, Privileged Access Manager uses the hard-coded default value (100 MB). If you use a value that is greater than the upper limit, Privileged Access Manager uses the upper limit value.  
**Type:** REG\_DWORD  
**Limits:** 1 - 2000 MB  
**Default (DMS\_\_ and DH\_\_WRITER):** 1024 MB  
**Default (all other PMDBs):** 100 MB
- **UseEncryption**  
Specifies whether update information that is saved to the updates.dat file is encrypted.  
**Values:** 0Do not encrypt the updates.dat file, 1encrypt the updates.dat file  
**Default:** 0

## endpoint\_management key

Privileged Access Manager maintains specific DMS Endpoint Management settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\  
DMS_NAME\endpoint_management
```

dmsmgr defines the registry values in this key when it creates a DMS. This key is not defined if a DMS does not exist on the host.

The Pmd\DMS\_Name\endpoint\_management registry key contains the following registry entries:

- **AutoSync**  
Specifies to automatically synchronize the Distribution Host with the Message Queue server.  
**Limits:** 0,1  
**Default:** 0 (disabled)
- **commands\_to\_exec\_before\_sleep**  
Specifies the number of endpoint commands that the DMS executes in a loop before sleeping.  
**Default:** 10
- **debug\_mode**

Specifies if Privileged Access Manager writes debug messages to the endpoint\_management.log file in the DMS directory (1).

**Limits :** 0,1

**Default :** 0 (debugging is disabled)

#### NOTE

The log file is located at *DMS\Install\Directory\endpoint\_management.log*

- **deployment\_lifetime**  
Specifies the deployment lifetime in days. Older deployments are removed at 2 am. To disable deployment cleanup, set this value to 0.  
**Default:** 30 days
- **operation\_mode**  
Specifies whether central (DMS) endpoint management through the Privileged Access Manager Message Queue is enabled.  
**Limits:** 0,1  
**Default:** 1 (enabled)
- **sleep\_between\_exec\_commands**

#### NOTE

Specifies the length of time, in milliseconds, that the DMS sleeps. When the DMS wakes it performs the number of endpoint commands specified in the commands\_to\_exec\_before\_sleep registry value. Default: 100

## policyfetcher (Windows)

Privileged Access Manager maintains policyfetcher service settings it uses under the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\policyfetcher`

The policyfetcher registry key contains the following registry entries:

- **check\_deployment\_tasks**  
Defines how often, in seconds, policyfetcher checks for new deployment tasks (DEPLOYMENT resources) on the Distribution Host.  
**Default:** 3600 (every 10 minutes)
- **deploy\_timeout**  
Defines the number of seconds policyfetcher waits for a deployment or undeployment task to complete on the endpoint.  
**Default:** 900
- **devcalc\_command**  
Defines the selang command that policyfetcher uses to run the deviation calculation.  
**Default:** start DEVCALC params(-nonotify)  
**Example:** start DEVCALC params(-nonotify -precise)
- **dh\_command\_retry\_interval**  
Defines the number of seconds between each DH notification command retry.  
**Default:** 60
- **endpoint\_heartbeat**  
Defines the frequency at which policyfetcher sends a heartbeat to the Distribution Host (DH). The frequency is a factor of the check\_deployment\_task setting, and determines how many times policyfetcher checks deployment tasks before it sends a heartbeat. For example, if check\_deployment\_task is set to the default 600 seconds (10 minutes) and you set this to 6, policyfetcher sends a heartbeat every 3600 seconds (1 hour).  
After sending the heartbeat, the policyfetcher also runs the deviation calculator (start devcalc command) and then waits 60 seconds for the deviation calculation to complete. After 60 seconds, policyfetcher continues to check that local endpoint information is identical to DH information.

**Default:** 6

- **max\_deployment\_errors**

Defines the maximum number of deployment errors that the endpoint sends to the DMS.

**Default:** 10

- **max\_dh\_command\_retry**

Defines the maximum number of times policyfetcher retries to get update notifications from DH before giving up.

**Default:** 10

- **max\_dh\_retry\_cycles**

Defines the maximum number of cycles policyfetcher retries to get update notifications from production DHs before moving to disaster recovery DHs.

**Default:** 5

- **policy\_verification**

Specifies whether policyfetcher verifies new deployment tasks on a backup Privileged Access Manager database before executing the tasks.

Valid values:

**1** - Run policy verification

**0** - Disable policy verification

**Default:** 0

- **policyfetcher\_enabled**

Specifies whether to run the policyfetcher service.

Valid values:

**1** - Run policyfetcher

**0** - Disable policyfetcher

**Default:** 1

## PUPMAgent Registry

Privileged Access Manager maintains the Shared Account Management Agent settings it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\PUPMAgent
```

The Shared Account Management Agent registry key contains the following registry entries:

- **EnableLogonIntegration**

Specifies that terminal integration is enabled.

**Limits:** 0, terminal integration is disabled; 1, terminal integration is enabled.

**Default:** 1

- **EnableRunAsInterface**

Specifies whether the Shared Account Management Agent is prompted for the target user password.

**Limits:** 0, the Shared Account Management Agent is not installed, 1 the Shared Account Management Agent is installed.

**Default:** 1

- **InterfaceName**

Defines the interface name that the Shared Account Management Agent uses to handle requests.

**Default:** PUPMAgentInterface

- **OperationMode**

Specifies the Shared Account Management Agent work mode.

**Limits:** 0, the Shared Account Management Agent is disabled and not running; 1, the Shared Account Management Agent is enabled, running but not logging data to trace files; 2, the Shared Account Management Agent is enabled, running, and logging data to trace files.

**Default:** 0

- **ProcessArgumentsReplacement**

Specifies whether the Shared Account Management Agent support Process Arguments Replacement.



**Limits:** 0,1

**Default:** 0

**Note:** If choose to support Process Arguments Replacement, that is, you set the value of this registry entry to 1, you must also enable the CMD Plugin. To enable the CMD Plugin, set the following registry entry to 1:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\plugins\CMDPlg\OperationMode

- **RegistrationInterval**

Defines the registration lifetime in days.

**Limits:** 0-365

**Default:** 7

**NOTE**

To not auto register the endpoint, set the Autoregister token to 0

## Report

Privileged Access Manager maintains sereport settings it uses under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Reports

The Reports registry key does not contain any registry entries. It contains registry subkeys for every report sereport produces.

**NOTE**

For information about registry entries for each of the reports sereport produces, see the [sereport utility](#).

## ReportAgent Registry

Privileged Access Manager maintains Report Agent settings that it uses under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent

The ReportAgent registry key contains the following registry entries:

- **audit\_enabled**  
Specifies whether you want to send endpoint audit data to the Distribution Server.  
**Values:** 0 no; 1 yes  
**Default:** 0
- **audit\_filter**  
Defines the full pathname to the file that contains filtering rules for audit records that the Report Agent routes to an external source (such as the Audit Log). This file determines which records the Report Agent routes.  
**Default:** *ACInstallDir\Data\AuditRouteFlt.cfg*
- **audit\_queue**  
Defines the name of the queue to which the Report Agent sends endpoint audit data.  
**Default:** queue/audit
- **audit\_read\_chunk**  
Defines the maximal audit records the Report Agent tries to collect in a single read of the audit files.  
**Limits:** A positive integer  
**Default:** 300
- **audit\_send\_chunk**  
Defines the maximal audit records that the Report Agent sends to the Distribution Server in each connection. When the number of audit records the Report Agent collects reaches this number, it sends these records to the Distribution Server.  
**Limits:** A positive integer

**Default:** 1800

- **audit\_sleep**

Define the length of time the Report Agent sleeps between generating audit reports.

**Limits:** A positive integer representing a number of seconds.

**Default:** 10

- **audit\_timeout**

Defines the cycle at which the Report Agent must send endpoint audit data to the Distribution Server. If this amount of time passes from the last send, the Report Agent sends audit data to the Distribution Server. The Report Agent does this data even if the number of records it collected is less than the audit\_send\_chunk value.

**Limits:** A positive integer representing a number of seconds.

**Default:** 300

- **interval**

Defines the interval, in minutes, at which Privileged Access Manager generates and sends reports to the Distribution Server.

The *schedule* setting defines the interval start time and the days it operates on. If the Report Agent starts later than a scheduled occurrence, it sends a report at the next calculated interval (from the schedule) and then at the defined intervals after that on scheduled days.

**Example:** If you have schedule=8:30@Mon,Tue, Wed, and interval=5 and the Report Agent loads on Tuesday at 8:47 am, the Report Agent generates and sends a report at 8:50 am. This is the earliest cycle calculated from the scheduled start using the 5-minute interval.

**Values:** 0 No interval (use scheduled occurrences only); *positive integer* number of minutes to use as interval

**Default:** 0

- **reportagent\_enabled**

Specifies whether reporting is enabled (1) on the local computer.

**Default:** 0

- **restart\_enabled**

Specifies restart of the ReportAgent daemon. Specify 1 to enable the restart.

**Default:** 0

- **schedule**

Defines when reports are generated and sent to the Distribution Server.

You specify this setting in the following format: time@day[,day2][...]

For example, "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

**Default:** 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

- **send\_queue**

Defines the name of the reporting queue on the Distribution Server to which the Report Agent sends snapshots of the local database and any PMDBs.

**Default:** queue/snapshots

## SeOSD Registry

Privileged Access Manager maintains generic settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSD
```

The SeOSD registry key contains the following registry entries:

- **AuditCollectorInterfaceName**

Defines the pipe name which functions as an audit interface between the audit collector component (within seosd) and the different clients of the audit collector (kernel).

**Default:** AuditCollector

- **AuditServerCacheSize**

Defines the size of the audit cache, in number of entries.

**Default:** 1024

- **CreateNewClasses**

Specifies whether you can add new classes, which are created with the seclassadm utility, to a Privileged Access Manager database.

**Default:** yes

- **CreateNewProps**

Determines whether you can add new properties, which are created with the sepropadm utility, to a Privileged Access Manager database.

**Default:** yes

- **dbdir**

The directory in which the Privileged Access Manager database is located.

**Default:** *AC/InstallDir\data\seosdb*

- **DefLookupThreads**

Defines the number of threads that Privileged Access Manager can use to resolve SIDs into account names.

**Default:** 5

- **DefLookupTimeout**

Defines the timeout, in milliseconds, before Privileged Access Manager stops trying to resolve an SID into an account name.

**Default:** 2000

- **domain\_names**

The list of name suffixes used for matching purposes.

Privileged Access Manager appends these suffixes to short host names to create long, fully qualified host names.

These names can be authorized in the relevant HOST, CONNECT, or TERMINAL classes. To identify a full name, Privileged Access Manager tries to append domain names in the domain\_names list to the short name for authorization purposes. For class HOSTNP, Privileged Access Manager matches all domain names (listed in this registry) with pattern to resolve into real IP addresses.

No default.

- **EnableCachedLogonInfo**

(Optional) Controls logon cache information in the CA ControlMinderSubAuth.dll and defines whether the product enables keeping data for authorization in runtime tables for performance tuning.

**Values:**

**0** - Logon caching is disabled. All logon events are passed to seosd for authorization.

**1** - Logon caching is enabled.

**Default:** 0

**NOTE**

This value is set to 1 when installing the Enterprise Management Server on a domain controller. After the upgrade, the value is restored to the same value as before the upgrade.

- **EnableIPv6Resolving**

Controls whether the host name to the IP address resolution is applied on IPv6 protocol in addition to IPv4.

**Values:**

**0** - Disables host name resolving over IPv6 protocol.

**1** - Enables host name resolving over IPv6 protocol.

**Default:** 0

- **EnablePolicyCache**

This value controls whether the authorization engine uses cached records or records directly from the database.

Valid values:

**no** - Authorization engine uses database records.

**yes** - Authorization engine uses cache records.

**Default:** no

- **EnvVarResolvingMode**

The method of resolving embedded environment variables (for objects in the FILE, SECFILE, PROGRAM, PROCESS, SPECIALPGM, TERMINAL, or USER classes). For example:

newfile %SystemRoot%\temp.txt. Privileged Access Manager does the following actions, depending on the value you select:

- 0** - Tries to resolve all environment variables, issues an error message to the user, and does not create the object.
- 1** - Tries to resolve all environment variables, issues a warning message to the user, and creates the object.
- 2** - Tries to resolve all environment variables and creates the object with no messages.
- 3** - Does not try to resolve environment variables.

#### NOTE

The PMDB assumes that there are no environment variables, so resolving is never tried. Default: 2

- **GeneralInterceptionMode**  
Specifies whether to use Full Enforcement mode (0) or Audit Only mode (1).  
**Default:** 0
  - **GraceCountForMessage**  
Defines the number of remaining grace logins at which the Change Password dialog appears.  
**Default:** 0
  - **HostResolutionMode**  
Specifies the method Privileged Access Manager uses to resolve host names.  
**Values:**
    - 0** - HOST resolution is synchronous (current behavior).
    - 1** - HOST resolution is asynchronous (with 'Event Log' reporting)

The effects of this setting are:

    - a. a. Control is returned to selang immediately.
    - b. If a HOST record cannot be resolved, a selang message is not displayed (same as 0).
    - c. A notification message is written into the 'Event Log'.  - 2** - HOST resolution is asynchronous (without 'Event Log' reporting).  
Same as '1' with the exception that notification messages are *not* written anywhere.  
**Default:** 0
- **HostResolutionRenewal**  
The time for internal cache refresh. The network interception authorization events use the registry value.  
**Default:** 30000
- **HostResolutionTimeout**  
The time the authorization engine waits for reverse IP lookup requests, upon network interception event.  
**Default:** 2000
- **LogonTimeOut**  
Defines the time in milliseconds Privileged Access Manager waits for transactions with the sub authentication DLL (eACSubAuth.dll) before giving up. When this time passes, Privileged Access Manager replies with the value set in LogonTimeOutAnswer.  
**Default:** 4000
- **LogonTimeOutAnswer**  
Defines the logon answer to the operating system when the LogonTimeOut setting elapses without an answer from Privileged Access Manager.  
**Default:** 1 (true)
- **MaximumDiscreteFILELimit**  
The number of discrete FILE records you can create in the Privileged Access Manager database.  
The minimum value is default; if a user sets this value to be less than the default, Privileged Access Manager acts as if a minimum were set.  
**Default:** 4096
- **MaximumGenericFILELimit**

The number of generic FILE records (name pattern-based records) you can create in the Privileged Access Manager database.

The minimum value is default; if a user sets this value to be less than the default, Privileged Access Manager acts as if a minimum were set.

**Default:** 512

- **ProcessCreationNotificationMode**

Specifies whether to intercept process creation and notify seosd either using kernel or instrumentation mode.

**Type:** REG\_DWORD

**Values:**

0 - Process creation is performed using kernel module

1 - Process creation is performed using instrumentation module

**Default:** 0

**NOTE**

If you set the key to 1, Privileged Access Manager intercepts process creation through the Windows API only.

- **RebuildSuspiciousDatabase**

This value is addressed only if database was not properly closed on previous session.

If the value is set to 0, the database is verified in a heuristic procedure for correctness (during startup). If the check finds a problem in the database, the database is rebuilt.

If the value is set to 1, the heuristic procedure check function is skipped. The database is rebuilt according to the database integrity check.

**Default:** 1

- **RefreshIPInterval**

The time (in minutes) between consecutive automatic IP refresh requests.

If the value is set to 0, IP refreshes are not automatically performed. If you use a value from 1 through 30, Privileged Access Manager uses 30 minutes, which is the minimum amount of time you can set, as the value.

**NOTE**

Refresh requests can be time consuming. For more information, see the secons utility -refIP option.

**Default:** 0

- **ResponseFile**

The location where the response.ini, used by eACOexist.exe utility, resides.

**Default:** *ACInstallDir\data\response.ini*

- **Service\_ACE\_Count** Specifies the list of service names that are protected and monitored by Privileged Access Manager. Each entry represents service name and its respective DACL count. The registry entry is updated by Privileged Access Manager internally.

- **sim\_login\_timeout**

Defines the timeout (in minutes) before Privileged Access Manager removes unused simulated login user entries from the Accessor Element Entry table (ACEE).

Privileged Access Manager simulates a login to create ACEE entries when it needs access to information that can be found in the ACEE.

**Default:** 60

- **SurrogateInterceptionMode**

Specifies the SURROGATE class interception mode.

**Type:** REG\_DWORD

**Limits:** 0 - user mode interception, Privileged Access Manager intercepts only the impersonation requests that originate from the RunAs utility; 1 - kernel mode interception, Privileged Access Manager intercepts all impersonation requests.

**Default:** 0

- **SusrauthReadParamsSec**

Defines how often trace parameters are updated.

**Default:** 30

- **SusrauthTraceDbgEnable**

Specifies whether tracing into DbgView or kernel debugger is enabled (1).

**Default:** 0

- **SusrauthTraceFileEnable**

Specifies whether tracing into a trace file (SusrauthTraceFileName) is enabled (1).

**Default:** 0

- **SusrauthTraceFileName**

Defines the full pathname to the trace file.

No default

- **TerminalSearchOrder**

Specifies how the authorization engine determines which TERMINAL record it verifies during the authorization process.

Values:

**name** - Authorization engine first looks for a TERMINAL record by name and if one is not found, it looks for an IP address match.

**nameonly** - Authorization engine looks for a TERMINAL record by name and if one is not found, ceases searching. It ignores TERMINAL records with an IP address format.

**IP** - Authorization engine first looks for a TERMINAL record by IP address and if one is not found, it looks for a name match.

**NOTE**

TERMINAL class supports generic rules that are defined by wildcards (IP address or host name pattern match). Generic rules are always verified after specific (full-name) rules. For example, if you set this to IP, seosd looks for a TERMINAL resource in the following order: complete IP address match, complete host name match, IP address pattern match, host name pattern match.

**Default:** nameonly

- **TermSrvTimeout**

Specifies the timeout (in milliseconds) that the authorization engine waits for the second consecutive login, upon a Terminal Services connection.

**Default:** 2000

**NOTE**

When a user logs in using a local account, Privileged Access Manager receives two login attempt notifications: the first from the local terminal and the second from the terminal server. If the user is assigned grace login count, two login attempts are logged and subtracted from the grace count. Therefore, Privileged Access Manager does not update the grace count with the second login if the login attempt occurred within the specified timeout period.

- **trace\_file**

The name of the file to which the trace messages are sent, if trace messages are requested.

**Default:** *ACInstallDir\log\seosd.trace*

- **trace\_file\_type**

Type of trace file.

If you do change the value of the value and a trace file exists, the existing trace file is saved with the file name extension .backup and then a new trace file is started in the format you specified.

**Default:** text

- **trace\_filter**

The name of the file that contains the filter data that is used to filter the trace messages. Specify the full path of the file.

**Default:** *ACInstallDir\log\trcfilter.ini*

- **trace\_space\_saver**

The amount of free space, in KB, to be left in the file system. When the amount of free space is less than this number, Privileged Access Manager disables the trace.

**NOTE**

Trace is never automatically enabled, even if more space becomes available later.

**Default:** 5120

- **trace\_to**

The destination of trace messages. Privileged Access Manager does the following, based on the value you select:

none - Does not generate trace messages.

file - Generates trace messages and sends them to the file listed in the registry trace\_file as soon as Privileged Access Manager becomes active.

stop - Generates trace messages during the period of service initialization. Once the service is initialized, no more trace messages are generated.

**Default:** file, stop

## SeOSWD

Privileged Access Manager maintains watchdog settings that are used under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSWD

The SeOSWD registry key contains the following registry entries:

- **PgmRest** Specifies the period, in seconds, after the last event and before checking programs again. The program rests to prevent system overload.

**Default:** 10

- **PgmTestInterval**

The period, in seconds, between rescanning of programs.

**Default:** 18000

- **ProcDumpCreate**

Specifies if process mini dump is generated (1) or not (0) on restart service that reached the threshold.

**Default:** 0

- **ProcHandlesCritical**

Specifies the process critical handle count. The watchdog restarts the process when the critical handle count exceeds.

**Values:** 0 (disables token), 800 (minimum value)

**Default:** 1500

- **ProcHandlesHigh** Specifies the high watermark for the process handle count. The watchdog restarts the process during the restart hours when the defined handle count exceeds.

**Values:** 0 (disables token), 800 (minimum value)

**NOTE**

The *ProcHandlesHigh* registry key is disabled when the value is greater than *ProcHandlesCritical* value.

**Default:** 1000

- **ProcRestartHours** Specifies the hours when the watchdog restarts the high handle count process.

**Values:** 0 - 23 (value in hours)

**Default:** 0 - 5

- **ProcVSizeCritical** Specifies the process critical memory size in megabytes. The watchdog restarts the process immediately when the specified limit exceeds.

**Default:** 500 MB

- **ProcVSizeHigh** Specifies the high watermark for process memory size. The watchdog restarts during the restart hours.

**Default:** 300 (value in megabytes)

- **ProcVSizeInterval**

Specifies the interval, in seconds, between the process performance counters verification for services that the watchdog checks.

**Default:** 900 seconds

- **SecFileRest**

Specifies the period, in seconds, after the last event and before checking secured files again. The program rests to prevent system overload.

**Default:** 10

- **SecFileTestInterval**

The period, in seconds, between rescanning of secured files.

**Default:** 36000

- **WatchdogRequestsInterfaceName**

Specifies the pipe server name which communicates with the watchdog.

**Default:** WatchdogRequests

## STOP

Privileged Access Manager maintains Stack Overflow Protection (STOP) settings it uses under the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\STOP`

The STOP registry key contains the following registry entries:

- **STOPIniFileName**

Defines the full path and name of the STOP initialization file. This file contains the list of functions for which STOP is enabled.

**Default:** *ACInstallDir\Data\stop.ini*

- **STOPLearningModeEnabled**

Specifies whether STOP runs in a special learning mode. In this mode, incidents are logged but always permitted. That is, a denial incident is logged appropriately, but is permitted to continue.

**Default:** 0 (disabled)

- **STOPLogFileName**

Defines the full path and name of the dynamic incident database for stack overflow protection (STOP).

**Default:** *ACInstallDir\Log\STOPRTEvents.dat*

- **STOPServerTraceEnabled**

Specifies whether the STOP server module has trace logging enabled.

**Default:** 0 (disabled)

- **STOPSignatureBrokerName**

Defines the host name of the computer that (if defined) is used to retrieve STOP signatures database from. No default.

- **STOPSignatureFileName**

Defines the full path and name of the STOP signature file (a trusted incident database).

**Default:** *ACInstallDir\Data\stopsignature.dat*

- **STOPUpdateInterval**

Defines the period of time, in minutes, between two consecutive attempts to update the STOP signatures database.

**Default:** 60

- **STOPZeroSnapshotBypassEnabled**

Specifies whether STOP should permit incidents with a zero-size code snapshot.

**Default:** 0 (not permitted)

## Tracer

Privileged Access Manager maintains tracing module settings it uses under the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Tracer`



The Tracer registry key contains the following registry entries:

- **TraceCfgFile**  
Defines the full path of the file containing the initialized configuration settings for tracing Privileged Access Manager modules.  
**Default:** *ACInstallDir\Data\tracer.ini*
- **TraceEnabled**  
Specifies whether to enable the Trace mechanism.  
**Default:** 0 (disabled)

## uxauth Key Registry Settings

UNIX Authentication Broker maintains Active Directory schema settings that it uses under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth
```

UNIX Authentication Broker installs this registry key when you install the Privileged Access Manager UNIX Attributes plug-in on an Active Directory server. This registry key is not installed as part of Privileged Access Manager.

### NOTE

The default attributes are for the Active Directory 2003 R2 schema.

The uxauth registry key contains the following registry entries:

- **group\_gid\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the GID for a migrated UNIX group.  
**Default:** gidNumber
- **Trace\_Enabled**  
Specifies if tracing is enabled for the Privileged Access Manager UNIX Attributes plug-in.  
**Values:** 0 tracing is disabled, 1 tracing is enabled  
**Default:** 0
- **user\_gecos\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the geocos property for a migrated UNIX user.  
**Default:** geocos
- **user\_gid\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the GID for a migrated UNIX user.  
**Default:** gidNumber
- **user\_homedir\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the home directory property for a migrated UNIX user.  
**Default:** unixHomeDirectory
- **user\_loginshell\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the login shell property for a migrated UNIX user.  
**Default:** loginShell
- **user\_uid\_attr\_name**  
Specifies the Active Directory attribute to which UNIX Authentication Broker maps the UID of a migrated UNIX user.  
**Default:** uidNumber

## WebService

Privileged Access Manager maintains Web Service settings that it uses under the following key:

---

HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService

### NOTE

The WebService registry key and related entries are added as part of the Privileged Access Manager Endpoint Management installation.

The WebService registry key contains the following registry entries:

- **auditFileCheckInterval**  
Defines how often, in seconds, the Privileged Access Manager Web Service checks if the audit file size has reached the defined limit.  
**Default:** 60
- **auditFileMaxSize**  
Defines the maximum size in KB of the Privileged Access Manager Web Service audit log file.  
When the file reaches this size, the Web Service renames the file to "*Backup\_of\_logFileName*" and it creates an audit log file.  
**Default:** 20000
- **backLog**  
Defines the maximum size of the request queue the Privileged Access Manager Web Service maintains.  
**Default:** 101
- **localPortNumber**  
Defines the port Privileged Access Manager Web Service uses to open a non-SSL listener to accept SOAP requests from the local machine.  
**Default:** 0
- **logFileName**  
Defines the name of the Privileged Access Manager Web Service audit log file name.  
If you leave this value empty string (""), the Web Service sends log messages to the terminal when you run the Web Service with the -debug option.  
**Default:** *ACServerInstallDir\WebService\log\WebService.log*
- **machineName**  
Defines the name of the computer the Privileged Access Manager Web Service is installed on.  
**Default:** 127.0.0.1
- **maxRequestsQueue**  
Defines the size of the global request queue of sockets.  
**Default:** 1001
- **maxThreads**  
Defines the number of threads Privileged Access Manager Web Service uses.  
**Default:** 7
- **portNumber**  
Defines the port Privileged Access Manager Web Service uses to communicate.  
**Default:** 5248
- **sessionTimeout**  
Defines the number of seconds before Privileged Access Manager Web Service terminates a session when there is no operation.  
**Default:** 601
- **StandAloneService**  
Specifies whether the Privileged Access Manager Web Service operates as a standalone service.  
If the Web Service operates as a standalone service, the service is not stopped or started when you use secons to stop or seosd to start Privileged Access Manager services. Instead, you use Windows native tools to start and stop the Privileged Access Manager Web Service.  
If the Web Service does not operate as a standalone service, the service is stopped and started when you use secons to stop or seosd to start Privileged Access Manager services. You cannot use Windows native tools to start and stop

the Privileged Access Manager Web Service. However, to use `seosd -start` to start the Privileged Access Manager Web Service, define the Web Service in the `AccessControl\AccessControlServices` registry entry.

**Values:** 1 Operates as a standalone service; 0 Does not operate as a standalone service

**Default:** 1

- **TraceEnabled**

Specifies if tracing is enabled for the Privileged Access Manager Web Service components.

**Values:** 0 tracing is disabled, 1 tracing is enabled

**Default:** 0

## Additional Registry Keys

You can also add or modify the following registry keys and values to change the way Privileged Access Manager performs:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableFileInterception`  
Specifies whether the file interception hooking is disabled (relevant functions are not initialized at boot time).  
**Type:** REG\_DWORD  
**Value:** 1 (disabled)**Note:** If this registry entry does not exist (the default), or is set to any value other than 1, file interception is initialized at boot time.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableNetworkInterception`  
Specifies whether network interception hooking is disabled (relevant functions are not initialized at boot time).  
**Type:** REG\_DWORD  
**Value:** 1 (disabled)**Note:** If this registry entry does not exist (the default), or is set to any value other than 1, network interception is initialized at boot time.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableProcessInterception`  
Specifies whether process interception hooking is disabled (relevant functions are not initialized at boot time).  
**Type:** REG\_DWORD  
**Value:** 1 (disabled)**Note:** If this registry entry does not exist (the default), or is set to any value other than 1, process interception is initialized at boot time.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableRegistryInterception`  
Specifies whether the registry interception hooking is disabled (relevant functions are not initialized at boot time).  
**Type:** REG\_DWORD  
**Value:** 1 (disabled)**Note:** If this registry entry does not exist (the default), or is set to any value other than 1, registry interception is initialized at boot time.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\use_wfp_perf`  
Defines performance improvement in network issues that are related to packets with zero payload.  
**Type:** REG\_DWORD  
**Default:** 1
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SeosDrv\Parameters\KernelBuffersSize`  
When the Privileged Access Manager kernel driver (`seosdrv.sys`) starts, it allocates, by default, memory for its internal use, according to the following formula:  $\text{number\_of\_buffers} = \text{amount\_of\_RAM}$  For example, 256 buffers are allocated for 256 MB of RAM. Each buffer is 4096 bytes long. If you want to control the number of buffers that `seos.drv` allocates, create this registry key and set the value to the number of buffers to allocate.  
**Type:** REG\_DWORD  
**Note:** 32 is the minimum number of buffers.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\EventMessageFile`  
Defines the pathname to the `seosdrv.sys` driver.  
**Type:** REG\_EXPAND\_SZ  
**Default:** %SystemRoot%\System32\drivers\seosdrv.sys
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\TypesSupported`  
A standard Windows entry that defines the bitmask of supported event types.  
**Type:** REG\_DWORD  
**Default:** 7
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DIIScanList`  
Defines a list of comma-separated DLLs (by name) that trigger injection by `cainstrm.sys`  
**Type:** REG\_SZ  
**Default:** No default
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DIIScanListRefreshPeriod`

Defines the interval, in seconds, for scanning the cainstrm registry entry.

**Type:** REG\_DWORD**Default:** 600

- HKEY\_LOCAL\_MACHINE\System\CCS\Services\Cainstrm\parameters\ExcludeProcess

Specifies processes by name to be excluded from native instrumentation by the driver.

**Type:** REG\_MULTI\_SZ**Default:** none

- HKEY\_LOCAL\_MACHINE\SYSTEM\CCS\Services\Cainstrm\Parameters

Specifies the Privileged Access Manager low-level instrumentation policy towards .Net assemblies.

**Type:** REG\_DWORD**Default:** 1 (1 implies that the instrumentation of .Net assemblies is enabled.)

- HKLM\SYSTEM\CurrentControlSet\Services\cainstrm\Parameters\DotNetOperationMode

Defines the Privileged Access Manager low-level instrumentation policy toward .Net assemblies.

**Type:** REG\_DWORD**Default:** 1 (1 enables the instrumentation of .Net assemblies. Any value different from 1 disables the instrumentation of .Net assemblies.)

## Trace Messages

In the log files, all messages begin with a date and time prefix, followed by an event-type word in uppercase and a symbol such as :, !, or >.

Symbol	Means
:	Privileged Access Manager was signaled for an event or performed an action.
>	Privileged Access Manager made an authorization decision resulting in D (Deny), P, (Permit), or BYPASS (The event did not require the interpretation of an access rule-for example, a setuid request to the same UID as the current UID.)
!	Privileged Access Manager detected an error-for example, a request from an unknown process.

## APIAUTH Messages

Message	Means
APIAUTH ! P=ppp U=uuu ChangePasswd(user) Error 0xerr	Process ppp, associated with user uu, wants to change the password of user. The result of this request was an error with its code specified in hex. Use the semsgtool utility to determine the nature of the error.
APIAUTH ! P=ppp U=uuu CheckPasswd(user) Error 0xerr	Process ppp, associated with user uu, wants to check the validity of a new password for user. The result of this request was an error with its code specified in hex. Use the semsgtool utility to determine the nature of the error.
APIAUTH ! P=ppp U=uuu Error, Unknown API Service nnn	Process ppp used the Application Interface and passed a service code that Privileged Access Manager Programming Interface does not support, probably because of user error. Check the cause of the error, correct the source, and recompile it.
APIAUTH ! P=ppp U=uuu GeneralResourceProc Error nnn >description	Process ppp, working under UID uu, issued a request to access a general resource; however, the specified resource cannot be resolved. Either the specified class is not defined or the specified access is not known, probably because of user error. Check your code, correct it, and recompile.

APIAUTH ! P=ppp U=uuu in VerifyCreate only for ROOT	Process ppp, working under UID uuu, issued a VerifyCreate request to build an ACEE. This operation is permitted only to multiuser processes that are associated with UID 0 (root). If the specified process is to run as a multiuser process, rerun the process under root authorities. If not, determine why the process issued the request.
APIAUTH P=ppp U=uuu in VerifyDelete only for ROOT	Process ppp, working under UID uuu, issued a VerifyDelete request to remove an ACEE. This operation is allowed only to multiuser processes that are associated with UID 0 (root). If the specified process is supposed to run as a multiuser process, rerun it under root authorities. If not, determine why the request was issued.
APIAUTH ! P=ppp U=uuu LoginProc Error nnn >description	Process ppp, working under UID uuu, requested to verify a user's login. The Privileged Access Manager login verification procedure failed. Contact your vendor's technical support.
APIAUTH ! P=ppp U=uuu NULL ACEE Error VerifyCreate (ACEEH=hhh)	A user process marked as server made a request to create an ACEE (probably as the server process was handling login for an accessor). The result is a NULL ACEE for one of the following reasons: <ul style="list-style-type: none"> <li>• The specified user is not defined in the central database.</li> <li>• The issuer of the VerifyCreate request did not provide all the information correctly.</li> <li>• The specified user is not allowed to log in.</li> </ul>
APIAUTH ! P=ppp U=uuu NULL ACEE Error VerifyDelete (ACEEH=hhh)	Process ppp, associated with user uuu, and which is probably marked as a 'server' process, has requested to delete the ACEE handle hhh (probably as part of handling the user's signoff). However, no ACEE is associated with this handle, so Privileged Access Manager cannot delete it.
APIAUTH P=ppp U=uuu Request with ACEEH=1 > New ACEEH=hhh	Process ppp, working under UID uuu, requested access to a general resource and supplied an ACEE handle of -1. Privileged Access Manager used the ACEE handle associated with the requesting process. This message is typical of single user processes that request access to a resource. No action is required.
APIAUTH ! P=ppp U=uuu VerifyCreate(ACEEH=hhh) Error nnn	Process ppp, working under UID uuu, issued a request to VerifyCreate (to build an ACEE). The VerifyCreate procedure failed. Contact your vendor's technical support.
APIAUTH > P=ppp U=uuu VerifyCreate DENY (Result= P D C ) string	The VerifyCreate request was denied for one of the following reasons: <ul style="list-style-type: none"> <li>• The specified user cannot login due to time or day rules</li> <li>• The user cannot work from the specified terminal</li> <li>• The specified password (if supplied) is incorrect</li> <li>• One of the reasons described in the messages that follow.</li> </ul>
APIAUTH > P=ppp U=uuu VerifyCreate OK (ACEEH=hhh)!	The VerifyCreate request was granted. An Accessor Environment Element (ACEE) was built in storage. Privileged Access Manager returned an ACEE handle (ACEEH) to the calling program. If the specified user is not defined to Privileged Access Manager, the function returned an ACEEH of -1.

APIAUTH ! P=ppp U=uuu VerifyDelete(ACEEH=hhh) OK Error 0xerr	Process ppp, associated with user uuu, which is probably marked as a 'server' process, has requested the deletion of the ACEE handle hhh (probably as part of handling the user's signoff). The result of the VerifyDelete request is either OK or error; if the latter, the error code appears in hex as err. Use the utility semsgtool to determine the nature of the error.
APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc, R=rrr, A=nnn) DENY (Result='D')Why ? detaileddenialreason	The request to access resource rrr of class ccc with access xxx was denied. If the ACEEH is -1, the denial was based on universal-access rules. If the ACEEH is not -1, the denial was based on the user associated with the specified handle. The second line provides a detailed reason for the denial.
APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc R=rrr, A=xxx) PASS	The request to access a resource rrr of class ccc with access xxx was granted. If the ACEEH is -1 (the user is not defined), the permission to access the resource was based on universal-access rules. If the ACEEH is not -1, the permission was based on access rules relating to the user associated with the specified handle.

## CONNECT Messages

Message	Means
CONNECT P=ppp U=uuu ACEEH=hhh from ipip port1 to socket 6000 host=iiii	A request to open a window on host <i>iiii</i> (X-Terminal or station) was made by process <i>ppp</i> associated with UID <i>uuu</i> . The port number is always 6000; all other TCP/IP connection requests are ignored by Privileged Access Manager.
CONNECT > P=ppp U=uuu from ipip port1 to socket 6000 host=iiii BYPASS	Privileged Access Manager bypassed the CONNECT request without interpreting access rules, because the program executing in process ppp is the registered XDM program.
CONNECT > Result P D C P=ppp ACEEH=hhh TERM=tttWhy ? detaileddecisiontext	The CONNECT result is D (Deny) or P (Permit). The second line provides a reason for the decision.

## ERROR Messages

Error	Means
ERROR ! Cannot fork. Errno nnn.	During initialization, Privileged Access Manager forks a few times to become a daemon. The fork request failed with the specified error number.  If you cannot determine the cause of the problem, contact your vendor's technical support.
ERROR ! Exec of Privileged Access Manager agent failed ddd	The Engine cannot start up the Agent daemon. Check that the seagent executable is located in the right place, usually <i>ACInstallDir/bin/seagent</i> . If this file exists in the correct location, report the problem to your vendor's technical staff. In the message text, <i>ddd</i> is the error number that Privileged Access Manager received from the operating system when trying to execute seagent.
ERROR ! Failed to get memory for LOGIN programsERROR ! Failed to get memory for NFS devicesERROR ! Failed to get memory for PRIV programsERROR ! Failed to get memory for XDM programs	These messages imply a severe shortage of memory. Either your computer does not meet the minimum memory requirements to run Privileged Access Manager, or a software bug was found. Contact your vendor's technical support.

ERROR ! Failed to get memory for PROC table	When seosd starts up, it must scan all the running processes to resolve all required information on each running process. seosd failed to allocate memory for this purpose; therefore, it terminates execution. This is caused by a severe memory shortage.
ERROR ! Failed to register login pgm programname	<p>During startup, Privileged Access Manager registers all executable files that are to be treated as login programs. The list of login programs are defined in the code for each operating system environment.</p> <p>The specified <i>programname</i> cannot be located on the file system during startup. Privileged Access Manager ignores the program and startup continues.</p>
ERROR ! Failed to register privileged pgm programname	<p>During startup, Privileged Access Manager registers all executable files that are to be treated as privileged programs. The specified <i>programname</i> cannot be located on the file system during startup. Privileged Access Manager ignores the program and startup continues.</p> <p>The list of privileged programs are defined in the code for each operating system environment.</p>
ERROR ! Failed to register XDM pgm programname	<p>During startup, Privileged Access Manager registers all executable files that are to be treated as XDM programs. The list of XDM programs is defined in the code for each operating system environment.</p> <p>The specified <i>programname</i> cannot be located on the file system during startup. Privileged Access Manager ignores the program and startup continues.</p>
ERROR No Memory for FileDb List	During startup, seosd cannot allocate memory to hold the list of protected files. This is probably due to a severe shortage of memory. The seosd daemon is terminated.
ERROR ! No Memory for GroupDb List ERROR ! No Memory for HostDb List ERROR ! No Memory for ServDb List ERROR ! No Memory for UserDb List	These messages imply a severe shortage of memory. Either your computer does not have the minimum memory required to run Privileged Access Manager, or a software bug was found. Contact your vendor's technical support.
ERROR ! PreMatureExec Assuming FORK Child=ppp Parent=PPP	<p>This message indicates that process ID (<i>ppp</i>) issued an EXEC system call, which is not known to seosd. Normally, such messages indicate that seosd was not yet informed of the FORK system call that preceded the EXEC request. It may indicate a problem in the serialization locks that the Privileged Access Manager extension to the UNIX kernel, SEOS_syscall, must maintain.</p> <p>If the <i>ppp</i> in the message text is the pid of seagent, you can ignore the message. If you get the message more than once, report the problem to your vendor's technical support.</p>
ERROR ! P=ppp Exec Failed	Privileged Access Manager received an EXEC event, but the inode number of the executable was zero. This message occurs when invoking a script file that does not contain the <code>#!/</code> shell-program declaration line at the beginning. No action is necessary.



ERROR ! Privileged Access Manager file table set failed	seosd attempted to set the file table (a table of all Privileged Access Manager protected files); however, SEOS_syscall refused this request. The most likely causes are insufficient memory in the kernel, or different versions of seosd and SEOS_syscall. Privileged Access Manager file protection cannot continue to function properly.  If you can, resolve the version mismatch. If everything looks fine, report the problem to your vendor's technical support.
ERROR ! seosini_ShutDown rv=errorno	Privileged Access Manager encountered an error during shutdown. Report the error to your vendor's technical support.
ERROR ! String too general 'path'	An attempt was made to define a generic rule for file protection, probably through a newfile or newres FILE command. However, the specified path cannot be a generic file access rule. The file rule is not defined.
ERROR ! Unknown request Type ttt Pid=ppp, Buff=bbb	Privileged Access Manager received a request from its system call, but the request type ttt is not recognizable. This can be due to a software version mismatch between the system call and seosd, or because of a software error. The request came from process ppp, and bbb is a printout of the request buffer. Report the problem to your vendor's technical support.

## EXEC Messages

Message	Means
EXEC P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm ProgramName Attached to ipaddress	Privileged Access Manager received a program execution event from process ppp associated with UID uuu and GID ggg. (A ggg value of -1 indicates that Privileged Access Manager has not yet registered the GID of that process). In the message text, ddd and iii are the file's device number and inode, respectively. Program-Name is the zero argument used when invoking the program. The specified program is a regular program (that is, not setuid or setgid); therefore, Privileged Access Manager grants its execution without invoking the database access rule decision mechanism. If the ip-address to which the process is attached is extractable, Privileged Access Manager reports this in the message text.
EXEC sg P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm ProgramName Attached to ipaddress	Privileged Access Manager received a program execution event from process ppp associated with UID uuu and GID ggg. (A ggg value of -1 means Privileged Access Manager has not yet registered the GID of that process). In the message text, ddd and iii are the file's device number and inode, respectively. Program-Name is the zero argument used when invoking the program. The specified program is a setgid program; Privileged Access Manager determines whether to grant its execution by invoking the database access rule decision mechanism. If the ip-address to which the process is attached is extractable, Privileged Access Manager reports this in the message text.



EXECsu P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm ProgramName Attached to ipaddress	Privileged Access Manager received a program execution event from process ppp associated with UID uuu and GID ggg. (A ggg value of -1 means Privileged Access Manager has not yet registered the GID of that process). In the message text, ddd and iii are the file's device number and inode, respectively. Program-Name is the zero argument used when invoking the program. The specified program is a setuid program; Privileged Access Manager determines whether to grant its execution by invoking the database access rule decision mechanism. If the ip-address to which the process is attached is extractable, Privileged Access Manager reports this in the message text.
EXECsusg P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm ProgramName Attached to ipaddress	Privileged Access Manager received a program execution event from process ppp associated with UID uuu and GID ggg. (A ggg value of -1 means Privileged Access Manager has not yet registered the GID of that process). In the message text, ddd and iii are the file's device number and inode, respectively. Program-Name is the zero argument used when invoking the program. The specified program is a setuid and setgid program; Privileged Access Manager determines whether to grant its execution by invoking the database access rule decision mechanism. If the ip-address to which the process is attached is extractable, Privileged Access Manager reports this in the message text.
EXEC > P=ppp U=uuu (R=rrr E=eee S=sss) to (E=EEE) BYPASS	Although the program is setuid, setgid, or both, and its execution should have invoked the access rule decision mechanism, Privileged Access Manager bypassed this check because the owner of the file EEE is the same as the current effective UID (eee). The program execution cannot change the scope of the privileges of the process. If the program is defined in the database as a trusted program and was modified or otherwise tampered with, program execution is not granted.
EXEC > Result 'R' stage=sss gstag=ggg ACEEH=hhh rv=rc Why? DetailedDecisiontext	Privileged Access Manager checked the authority of the user to execute the program and the result R, where R is either D (deny) or P (permit). The stage sss and the granting-stage ggg indicate which phase of the decision flow determined the result. The ACEE handle hhh was used as the accessor to the program. If the result is 'C' (check) it means Privileged Access Manager did not make a decision, probably because of a software error-contact your vendor's technical support and provide them with the return value rc. Detailed-Decision-text is a textual description of the stage and granting-stage. If the result was P, the program is executed successfully. If the result is D, the program will not be executed and the user receives a permission denied message.
EXECARGS 'execution arguments'	Because of an EXEC syscall, Privileged Access Manager displays the executed command line with all the arguments passed to it.

## FILE Messages

Message	Means
FILE P=ppp U=uuu (D=dev I=inode) acc pathname	Process ppp associated with userid uuu attempted to access a Privileged Access Manager protected file. In the message text, dev and inode are the device and inode of the file being accessed, respectively; acc is the access mode (that is, READ, WRITE, and so on); and pathname is the real path name of the file being accessed.

FILE > Result 'D' Privileged Access Manager File Only 'filename'	The result of the file access request is D (denial) because only Privileged Access Manager can access this file. Even if the access rules permit access, Privileged Access Manager is hard-coded to deny access to this file.
FILE > Result 'R' stage=sss gstag=gs ACEEH=hhh rv=rv (recordname)Why? detailedreasonstext	The result R of the file access request is either D (deny) or P (permit). The stage sss and granting stage gs are mapped to a text-string reason, on the second line (following Why?). In the message text hhh is the accessor handle associated with the request's accessor and record-name is the name of the access rule record that triggered the decision to deny or permit access.

## INET Messages

Message	Means
INET P=ppp, from ipaddress localport to port portnumber	Privileged Access Manager intercepted an incoming Internet accept request that was issued by the remote ip-address requesting the TCP/IP service port-number.
INET > Result 'R' ipaddr>locport, stg=stage gtsg=gstageWHY ? DetailedReasonText	The result R of the Internet request is P (permit) or D (deny). In the message text, ip_addr is the IP address of the request. Detailed-Reason-Text is the textual description that indicates which stage and granting stage phase of the decision flow made the final decision to deny or allow the TCP/IP service for the requesting host.

## INFO Messages

Message	Means
INFO AutoDisabling Tracedue to tight fsspace (space)	The trace facility automatically disables itself when the amount of free space left in the file system where the trace file resides, goes below a threshold specified by the trace_space_saver token in the seos.ini file. In the message text, space is the amount of free space left on the file system.
INFO Can't fetch fs freespace (errno=err)	The Auto Disable feature of the trace facility cannot determine the amount of free space in the file system. In the message text, err is the error integer received from the UNIX statfs() call. Report the problem to your vendor's technical support.
INFO DB Query	The seosd daemon received a request to extract information from the Privileged Access Manager database.
INFO DB Request	The seosd daemon received a request to modify or query data in the Privileged Access Manager database.
INFO Filter Mask 'mask' is registered	The seosd daemon registers each filter mask that is read from the trcfilter.init file, so that messages matching the mask are not sent to the trace file.
INFO GroupList Registered with nnn entries	When seosd runs under the NIS server, it caches all group entries (from /etc/group and NIS maps) at startup, so that seosd can solve GID to group name translations without invoking ypserv processes and TCP/IP requests. This message also indicates that the under_NIS_server token in seos.ini is set to YES. If the station where Privileged Access Manager is running is not the NIS server, set the under_NIS_server token to NO. In the message text, nnn is the number of group entries that were cached.

INFO HostList Registered with nnn entries	The seosd daemon caches all entries from /etc/hosts at startup. In the message text, nnn is the number of host entries cached.
INFO Login program programname is registered	The seosd daemon must recognize all the programs through which users log in to the system. Privileged Access Manager treats a setuid system call invoked by a login program as a login request, and not as a setuid request. In the message text, programname is the full path of the login program that was registered. The seosd daemon takes the names of the login programs internally, from the Privileged Access Manager startup code.
INFO NFS Device Majors Registered, nnn entries	The checks that the Watchdog performs for trusted programs include checking the device number on which the file resides. This check can lead to errors if the file resides on an NFS mounted file system-especially an auto-mounted file system-for which device numbers can have a different value after boot. For this reason, Privileged Access Manager registers the major device numbers of NFS file systems so that they can ignore the non-stable minor device number. Privileged Access Manager has a list of major device numbers for NFS mounted file systems in each environment. If your installation uses a network mounted file system that Privileged Access Manager does not recognize, contact your vendor's technical support for instructions about adding major device numbers to the list. In the message text, nnn is the number of major device numbers registered as NFS mounted file systems.
INFO P=ppp ended	Process ppp ended. seosd disassociates this process number from its ACEE (accessor environment element). If process ppp was the last process associated with its ACEE, (that is, no other parent processes or subprocesses use the same environment), then the ACEE is removed from storage. This message is not issued immediately after the process has terminated; it is issued only when Privileged Access Manager performs some garbage collection to reuse process entries in its internal tables.
INFO P=ppp Exec Failed	This message indicates that process ppp failed to execute the last EXEC syscall, because UNIX refused this request (after Privileged Access Manager granted the execution). Therefore, Privileged Access Manager restores the value of the former executable that was associated with this process, as the program running under this process ID. In most cases, the process terminates. This is not necessarily an error, and you need not take any special action. However, you should use UNIX tools to isolate the reason that execution failed. In most cases, the reason is that a shell script does not have the #!/bin/sh header on the first line.
INFO P=ppp Unknown TTY type typename	The seosd daemon cannot determine if the process ppp is using a real TTY or a pseudo TTY. Contact your vendor's technical support.
INFO Privileged program programname is registered	The seosd daemon registers a few privileged programs. Such programs are allowed to setuid to any user without checking the SURROGATE class. Currently, you can only make /bin/sendmail a privileged program, due to its flow requirements. You must keep this list as small as possible; we recommended that seoswd monitor all privileged programs to make sure they remain trusted. In the message text, programname is the full path of the registered program.

INFO Restricted File Table set with nnn entries	During startup, seosd found nnn entries for Privileged Access Manager protected files, and successfully passed this list to the Privileged Access Manager extension of the UNIX kernel. This is an information-only message.
INFO SEOS_syscall UnRegister rc=nnn	During shutdown, seosd unregisters itself to the kernel so that it can start up again. In the message text, nnn is the return code, which should be zero. If the return code is not zero, report the problem to your vendor's technical support.
INFO ServList Registered with nnn entries	The seosd daemon caches all entries from /etc/services at startup. In the message text, nnn is the number of host entries that were cached.
INFO ServList registered with nnn portmapper entries	While starting up, seosd registered nnn TCP/IP services that are resolved by the portmapper. This is an information-only message.
INFO Set site	The seagent daemon, the Privileged Access Manager daemon responsible for communication with other Privileged Access Manager stations, sent seosd a connection request from a remote station.
INFO Setting PV C=ccc O=ooo P=ppp	The seoswd daemon set the value of property ppp in object ooo of class ccc.
INFO UserList Registered with nnn entries	When seosd runs under the NIS server, it caches all user entries (from /etc/passwd and NIS maps) at startup, so that seosd can solve UID to user name translations without invoking ypserv processes and TCP/IP requests. This message also indicates the under_NIS_server token in seos.ini is set to YES. If the computer where Privileged Access Manager is running is not an NIS server, set under_NIS_server token to NO in seos.ini. In the message text, nnn is the number of user entries that were cached.
INFO XDM program programname is registered	XDM programs are those programs that display the userid and password box on X-terminals. XDM programs run under superuser, who usually cannot open windows on X-terminals. However, the XDM program must open a window on an X-terminal to present a box with the userid and password for the user to specify. seosd therefore bypasses terminal checking if the program issuing the CONNECT request is a registered XDM program.

## KILL Messages

Message	Means
KILL P=ppp U=uuu kill Process All Except (nn) (proclist)	Process ppp associated with user uuu attempted to kill all the processes listed in proclist (or all the processes except the processes in the list). In the message text, nn is the number of target processes.
KILL > Result 'R' stage=sss gstag=gs rv=rr ACEEH=hhhWhy? detailedreason-text	The result R of the kill event is either D (deny) or P (permit). In the message text, sss, gs, and rr are the stage, granting stage, and return value of the Privileged Access Manager decision routines, and hhh is the accessor handle associated with the kill event. The detailed-reason-text appears in the second line and is a derivation of the stage and granting stage codes.

## LOGIN Messages

Message	Means
LOGIN P=ppp User=uuu Terminal=ttt	The seosd daemon intercepted a login request from user uuu working on terminal ttt under process number ppp. A Login Result message should follow this message.
LOGIN > Result 'R' stage=stage gstage=gstage rv=nnn ACEEH=hhh Why ?detaileddenialreason	The result of the login request R is either D (deny) or P (permit). In the message text, stage and gstage are numbers indicating the phase in the Privileged Access Manager flow that made the decision to grant or deny the login request. If the login was permitted, hhh is the ACEE handle that is now associated with the issuing process. If the login was denied, hhh is set to -1 and a detailed-denial-reason appears in the second line. If the detailed-denial-reason relates to resource access (such as no rule granting access to resource), the resource in question is the terminal from which the user issued the login request.
LOGIN > Result 'D' Login Disabled for ALL	The login request was denied because login is currently disabled for all users.
LOGIN > Result 'D' Login Disabled for U=uuu	The login request was denied because login is currently disabled for the specific user. The reason can possibly be that this user is already logged in.

## SCONSOLE Messages

Message	Means
SCONSOLE Login Disabled For UID uuu	The Privileged Access Manager console utility, secons, issued a request to disable a login request for the userid uuu. From this point, login requests for the specified userid are denied.
SCONSOLE Login is already Disabled for U=uuu	The secons utility issued a request to disable login request for the userid uuu. However, login is already disabled for this userid.
SCONSOLE Login is not Disabled for U=uuu	The secons utility issued a request to re-enable login for the userid uuu. However, login is already enabled for this userid.
SCONSOLE Login Is Now Disabled	The secons utility issued a request to disable login for all users. From this point on, login requests by any user are denied.
SCONSOLE Login Is Now Enabled	The secons utility issued a request to re-enable login for all users. From this point on, login requests are allowed.
SCONSOLE Login ReEnabled for U=uuu	The secons utility issued a request to re-enable login for a specified user. From this point on, login requests for this specific user are allowed.
SCONSOLE No more space in Disabled Logins Table	The secons utility issued a request to disable login for a particular user. However, the login disable table is full. Contact your vendor's technical support.
SCONSOLE U=uuu is not allowed for operation	A user without the OPERATIONS attribute tried to use one of the secons switches that are not allowed for non-OPERATIONS users.
SCONSOLE U=uuu is not allowed to disable login for U=uuu2	The user uuu tried to disable login for user uuu2 through secons. However, only root and user uuu2 are allowed to disable login for uuu2.

SCONSOLE U=uuu is not allowed to Reenable login for U=uuu2	The user uuu tried to re-enable login for user uuu2 through secons. However, only root and uuu2 are allowed to re-enable login for uuu2.

## SGID Messages

Message	Means
SGID P=ppp U=uuu G=ggg to GGG (GROUP.groupname) ACEEH=hhh D=devnum I=inode	Process ppp, running with the authorities of UID uuu and GID ggg, issued a setgid system call for the GID GGG. Privileged Access Manager checks the authority of that process using the SURROGATE class and object GROUP.groupname, and uses hhh as the accessor handle for the request. In the message text, devnum and inode are the device and inode of the issuing program, respectively. A SGID Result message should follow this one.
SGID > P=ppp U=uuu (RG=rg EG=eg SG=sg) to (RG=trg EG=teg SG=tsg) () BYPASS	Privileged Access Manager granted the setgid request without checking any SURROGATE access rules. In the message text, ppp is the issuing process id; uuu is the userid associated with this process; rg, eg, and sg are the real, effective, and saved GID of that process; and trg, teg, and tsg are the target effective, real, and saved GID with which the setgid request was issued. The reason for the bypass is usually because the current real or saved GID is the same as the target GID, and therefore the setgid request does not change the security scope of the user.
SGID > Result 'R' stage=stage gstag=gstage ACEEH=hhh Why? detailedreason-text	Privileged Access Manager checked the setgid request against a SURROGATE access rule and the result R is P (permit) or D (deny). The decision was made on behalf of the accessor handle hhh. In the message text, detailed-reason-text is the reason for the denial or grant.

## SHUTDOWN and STARTUP Messages

Message	Means
SHUTDOWN! Request Denied. U=uuu not allowed to SHUTDOWN the Server	The userid uuu tried to shut down seosd using secons; however, profile of the user does not have the OPERATIONS attribute. The request was therefore denied.
SHUTDOWN Server going down upon operator's request	The seosd daemon started shutting down following a request from an authorized operator.
SHUTDOWN Terminating Privileged Access Manager daemon daemonname P=ppp RV=nnn	Privileged Access Manager terminated its daemon ppp as part of its shutdown process; Privileged Access Manager also shuts down seoswd and seagent.
STARTUP Privileged Access Manager daemon PID=ppp	The seosd daemon was started; its process ID is ppp.

## SUID Messages

Message	Means
SUID > P=ppp U=uuu (R=r E=e S=s) to (R=tr E=te S=ts) (reason) BYPASS	Privileged Access Manager granted the setuid request without checking any SURROGATE access rules. In the message text, ppp is the issuing process id; uuu is the userid associated with this process; r, e, and s are the real, effective and saved UIDs of process ppp; and tr, te, and ts are the target effective, real, and saved UIDs with which the setuid request was issued. The reason for the bypass is usually because the current real or saved UID is the same as the target UID, and therefore the setuid request does not change the security scope of the user. Other possible reasons are that the program issuing the setuid system call is a privileged program (in which case reason is For Priv), or that the issuing program is a login program that switches UIDs several times before and after the actual login ( in which case reason is specified as For Login).
SUID P=ppp U=uuu (R=r E=e S=s) to USER.username (R=tr E=te S=ts)D=devnum I=inode	Process ppp, running with the authority of userid uuu, issued a setuid system call to change the current real, effective, or saved UID to UID uuu. Privileged Access Manager checks the authority of that process using the SURROGATE class and object USER.username for that request. In the message text, devnum and inode are the device and inode of the issuing program, respectively. A SUID Result message should follow this one.
SUID > Result 'R' stage=stage gstag=gstage ACEEH=hhh rv=rv Why? detailedreasontext	Privileged Access Manager checked the setuid request against a SURROGATE access rule and the result R is P (permit) or D (deny). The decision was made on behalf of the accessor handle hhh. In the message text, detailed-reason-text is the reason for the denial or grant.

## WARNING Messages

Message	Means
WARNING Associate P=ppp ACEEH=hhh	Privileged Access Manager performs an association between a process and an accessor handle (ACEEH) for any fork request. This message indicates that the association cannot be performed, either because the handle hhh is -1 or because hhh is not a valid accessor handle. In the latter case, contact your vendor's technical support.
WARNING Can't verify P=ppp	This message follows an Unknown P= message that indicates a fork request from an unknown process. Privileged Access Manager tries to determine who the user is that UNIX associates with that user. This verification task cannot be completed. A possible reason is that the process has already terminated. If not, contact your vendor's technical support.
WARNING DeAssociate P=ppp ACEEH=hhh	Privileged Access Manager performs a dissociation between a process and an accessor handle (ACEEH) for any process that is terminated. This message indicates that the dissociation cannot be performed, either because the handle hhh is -1 or because hhh does not exist as a valid accessor handle. In the latter case, report the problem to your vendor's technical support.

WARNING ExecArg for entry with P=ppp not NULL	This warning appears when the product finds a new process that was not known to the system, and for which the executing program is not known. In most cases, you can ignore the message. If the system does not produce the expected results, contact your vendor's technical support.
WARNING Failed to get ACEEH of P=ppp	Privileged Access Manager was requested to check the authority of process ppp but there was no valid accessor handle for that process. In most cases, the reason is that the user who is associated with the process is not a Privileged Access Manager defined user, or that the process is unknown to the product. In both cases, the product gives this process only universal access rights. If the system does not produce the expected results, contact your vendor's technical support.
WARNING Login for P=0 ???	When this message appears during startup in systems other than AIX, you can ignore it. If it appears during normal work (after seosd is started and functions), or during startup under AIX, then it identifies a software error, in which case you should contact your vendor's technical support.
WARNING CA PAMSC failed to kill P=ppp reason=nnn	As a measure of caution, the product kills processes trying to get sensitive privileges that may create loopholes. Such events can be attempts to surrogate the UID (setuid system-call) with no permission. Privileged Access Manager attempted to kill the violating process, but failed to do so. The reason for the failure is detailed in the reason code that is returned by the kill system call.
WARNING Terminal for entry with P=ppp not NULL	This warning appears when the product finds a new process that was not known to the system and for which the executing program is not known. In most cases, you can ignore the message. If the system does not produce the expected results, contact your vendor's technical support.
WARNING Unknown P=ppp	This message indicates a fork request that was issued by a process that is not known to the product. If this message appears for seoswd or seagent during startup, you can ignore it. At other times, it can imply a software error because the product cannot verify the actual authority of that process. For the latter case, contact your vendor's technical support.

## WATCHDOG Messages

Message	Means
WATCHDOG Ask if I'm Here (AYT)	The seoswd daemon tried to verify whether seosd is alive and give the expected response. In the message text, AYT is the seoswd are you there challenge. You can and should ignore this message; filter it out using the trcfilter.init file. The message implies normal behavior of seoswd.
WATCHDOG Init initializationtext	The seoswd initialization message, which you can ignore.
WATCHDOG Log logtext	The seoswd daemon issued a log request. The log request is detailed in log-text.



WATCHDOG SecFile operation result	The seoswd daemon requested the daemon to extract information regarding secured files. In the message text, operation can be GETFIRST or GETNEXT; the result can be OK if such information was extracted, or NOFOUND if there are no more secured files in the product database. This message signifies normal behavior of seoswd to scan secured files.
WATCHDOG Timer	The seoswd daemon issues a timer request every few seconds (as set by the seos.ini file). You can and should filter out this message using the trcfilter.init file.
WATCHDOG Trust Pgm programname OK NOTOK	The seoswd daemon marked the specified program as a trusted program. This implies that the specified program passed the digital signature tests. In the message text, OK means the trust operation completed successfully, and NOTOK means that seoswd failed to mark the program as trusted. The reason for NOTOK is probably a corrupted database, in which case you should contact your vendor's technical support.
WATCHDOG Untrust Pgm programname OK NOTOK	The seoswd daemon marked the specified program as untrusted. This implies that the specified program did not pass the digital signature checks of seoswd. In the message text, OK means that the untrust operation has completed successfully, and NOTOK means that seoswd failed to mark the program as untrusted. A possible reason for NOTOK can be a corrupted database, in which case you should contact your vendor's technical support.

## Other Trace Messages

Message	Means
ACTION CA ControlMinder killed P=ppp	Privileged Access Manager denied a setuid or login request and killed the requesting process (ppp) as a precautionary measure.
ALARM ! Uid uuu breached the system!!!	An unknown process made a request such as fork, exec, or setuid. The process is unknown to Privileged Access Manager and the UID assigned to the process is not assigned to any other process in the system. This implies that the user logged in without Privileged Access Manager being notified. This situation can occur as a result of a software bug or if the user logged in immediately after the product scanned the current process status but before completing initialization.
EXIT Going down...	Privileged Access Manager started the shutdown process and disabled the interception of system calls.
FATAL ! in seosrt_InitDatabase (nnn) Layer = nnn Stage = nnn Return Code = 0xnnn	Privileged Access Manager cannot initialize the database I/O routines. The possible reasons are: <ul style="list-style-type: none"> <li>No database in the directory is identified by the dbdir token in the seos.ini file.</li> <li>The user invoking Privileged Access Manager is not root.</li> <li>The database is corrupt.</li> </ul> If you cannot correct the problem, contact your vendor's technical support.

FORK P=ppp U=uuu G=ggg Child=cppp Pgm ProgramName	Privileged Access Manager intercepted a fork request made by process ppp associated with UID uuu and GID ggg. The child process id is cppp. Program-Name is the program running in the parent process (and, initially, also in the child process). The product never denies a fork request; it is always granted. Variations of the fork system call, such as vfork and kfork, are also reported as fork requests.
GETCRED P=ppp, Get Credentials by Ticket	This is an information-only message, which indicates that ppp (usually the process ID of the Policy Model daemon, sepmdd) requested the credentials of a specific ticket holder (a client process that requests the services of sepmdd). For more information, see the description of GTICKET in this appendix, and the description of sepmdd in the chapter Utilities in Detail.
GPEERNAM P=ppp, ADDR=addr, N=desc	Privileged Access Manager intercepted the getpeername() system call to verify which IP address is associated with the current process. This system call is always granted. In the message text, ppp is the process id issuing the getpeername() call and addr is the IP address associated with the socket descriptor desc.
GTICKET P=ppp, Get Authentication Ticket	This is an information-only message, which indicates that ppp requested seosd to issue an authentication ticket for it. Whenever the Policy Model client, sepmdd, communicates with sepmdd, the server verifies the identity of the client through the passed ticket. The client sends the acquired ticket to the server using socket communication. The server then passes this ticket to seosd to get the credentials of the ticket holder with the GETCRED request. In this way, sepmdd ensures the identity of the client requesting its services.
MESSAGE string	A marker message is placed in the trace file by console request.
NEWPASS Set new password	The sepass utility requested to set a new password for a user id.
PW_ATTCK P=ppp make nnn attempts in sss seconds from terminal	The seosd daemon detected that process ppp, which is running one of the registered login programs, made nnn attempts to specify a user/password combination with no success. Privileged Access Manager concluded that a password guess attack originated at the terminal specified in the message text, and wrote an audit record to the audit file. PWATTACK audit records can trigger actions by the log routing daemons (selogrcd and selogrd).
RESTART DBSERV restarted by Watchdog (P=ppp)	The seoswd daemon has restarted seosd. In the message text, ppp is the process ID of seosd.
SETGRPS P=ppp to grouplist	The process ppp issued the setgroups system call for the groups specified in grouplist.
STREAM c P=ppp Closes Stream Id=iii	Process ppp closed a stream with stream ID iii. Privileged Access Manager keeps track of all stream-open and stream-close operations to determine later-when a TCP/IP request is processed on behalf of a specific stream-id-which process ID owns the stream.
STREAM o P=ppp Opens Stream Id=iii	Process ppp opened a stream with stream ID iii. Privileged Access Manager keeps track of all stream-open and stream-close operations to determine later-when a TCP/IP request is processed on behalf of a specific stream-id-which process ID owns the stream.
VERPASS Verify password	Privileged Access Manager received a request to verify password validity for a user.
WAKE_UP Server going up	The seosd daemon started to initialize.

## PAM SC Communication Ports

This section contains detailed information on the communication ports that are used by the PAM SC components.

Use the table of contents to access the topics in this section.

### PAM SC UNIX Endpoint Used Ports

The following table lists and describes the ports used by PAM SC UNIX endpoints.

Port Number	Description	Direction	Protocol	Source	Target	Comments
8891	PAM SC Client Applications	Incoming	TCP	Remote PAM SC Utilities	PAM SC Agent	You can change the default port number by modifying the <code>/etc/services</code> file settings. To modify the default port number, add the following line, then restart PAM SC daemons:  <pre>seoslang2   port- number/ tcp</pre>
5249	SSL Communications	Incoming	TCP	Remote PAM SC Utilities	PAM SC Agent	FIPS 140-2 compliant. For more information about SSL communication, see the SSL, Authentication, and Certificates section in the <i>Implementation Guide</i> .

8892	Starting seosd from a remote computer	Incoming	TCP		seosload	<p>When seload loads daemons on a remote computer, inetd (internet services daemon) on the remote computer executes the rseload program. This program executes seload locally and exits; it receives the parameters on this port. You can change the default port number by modifying the /etc/services file settings. To modify the default port number, add the following line, then restart PAM SC daemons:</p> <pre>seosload     port- number/ tcp</pre> <p><b>Note:</b> The communication on this port is not encrypted since it does not send any sensitive information.</p>
61616	Reports and Audit Events	Outgoing	TCP	ReportAgent	Distribution Server	
8891	PAM SC Client Applications	Outgoing	TCP	Policyfetcher	Distribution Server	Distributing AC policies to endpoints through Advanced Policy Management.
5249	SSL Communications	Outgoing	TCP	Policyfetcher	Distribution Server	Distributing AC policies to endpoints through Advanced Policy Management when SSL is enabled.

## Windows Endpoint Used Ports

Privileged Access Manager uses the following TCP ports on Windows by default:

Port Number	Description	Direction	Source	Target	Comments
8891	Privileged Access Manager client applications	Incoming	selang.exe, sepmdd.exe (PMD), eACSigUpdate.exe, SegraceW.exe (grace login and password settings), secons.exe (remote shutdown and IP address refresh), policydeploy.exe, devcalc.exe, policyfetcher.exe	CA ControlMinder Agent	You can change the default port number by modifying the %SystemRoot%\drivers\etc\services file settings. To change the default port number, add the following line, then restart Privileged Access Manager services:  seoslang2 port-number/ tcp
5249	SSL Communications	Incoming	For information about the components which provide FIPS-compliant communications, see the Release Notes.	CA ControlMinder Agent	FIPS 140-2 compliant
61616	Reports and audit events	Outgoing	ReportAgent	Distribution Server	
8891	Privileged Access Manager Client Applications	Outgoing	Policyfetcher	Distribution Server	Distributing AC policies to endpoints through Advanced Policy Management.
5249	SSL Communications	Outgoing	Policyfetcher	Distribution Server	Distributing AC policies to endpoints through Advanced Policy Management when SSL is enabled.

## Default TCP Ports Used by PAM SC Server Components

Privileged Access Manager uses the following TCP ports for its server components by default:

Port Number	Description	Direction	Source	Target
61616	Report snapshots using SSL	Outgoing	Enterprise Management Server	Utility Appliance
5248	Local web-based interface communications	Outgoing	Enterprise Management	Web Service
9095	Used for login integration from PAM SC	Outgoing		Utility Appliance

9091	Policy orchestration from PAM SC	Outgoing		Utility Appliance
------	----------------------------------	----------	--	-------------------

In addition to the default ports, you may need to open the following ports:

- On the computer of the central database for communication with the Privileged Access Manager Enterprise Management, if these components are on separate computers.
- On the Report Portal (BusinessObjects) computer to access the InfoView application from remote computers (8080 by default).
- On the Privileged Access Manager Endpoint Management and Privileged Access Manager Enterprise Management computer to access the web-based interfaces from remote computers (18080 by default).
- On the computer where you install Oracle Database to access the web-based interface from remote computers (by default, 8080 or 61616 for SSL).
- On the computer of the central database for communication with the PAM Server Control Enterprise Management, if these components are on separate computers.
- On the Report Portal (BusinessObjects) computer to access the InfoView application from remote computers (8080 by default).
- On the PAM Server Control Endpoint Management and PAM Server Control Enterprise Management computer to access the web-based interfaces from remote computers (18080 by default).
- On the computer where you install Oracle Database to access the web-based interface from remote computers (by default, 8080 or 61616 for SSL).

## UNIX Authentication Broker Used Ports

UNIX Authentication Broker uses the following TCP ports on UNIX by default:

Number	Description	Source	Target
53	DNS	UNIX Authentication Broker Agent	Active Directory
88	Kerberos traffic	UNIX Authentication Broker Agent	Active Directory
389	Kerberized LDAP	UNIX Authentication Broker Agent	Active Directory
445	Microsoft directory services	UNIX Authentication Broker Agent	Active Directory
464	Kerberos kpasswd	UNIX Authentication Broker Agent	Active Directory
3268	Global Catalog	UNIX Authentication Broker Agent	Active Directory
61616	Report snapshots using SSL	Report Agent	Utility Appliance

UNIX Authentication Broker uses the following UDP ports on UNIX by default:

Number	Description	Source	Target
53	DNS	UNIX Authentication Broker Agent	Active Directory
88	Kerberos traffic	UNIX Authentication Broker Agent	Active Directory

123	NTP	UNIX Authentication Broker Agent	Active Directory
389	Kerberized LDAP	UNIX Authentication Broker Agent	Active Directory
464	Kerberos kpasswd	UNIX Authentication Broker Agent	Active Directory

## Endpoint Management Used Ports

Privileged Access Manager uses the following TCP ports to manage automatically registered endpoints by default:

Number	Description	Direction	Source	Target	Comments
135	Remote Procedure Call	Incoming	Distribution Server	Windows Endpoints	Remote Procedure Call (RPC) needed for WMI.
445	Remote registry access	Incoming	Distribution Server	Windows Endpoints	Remote registry access that is needed for WMI.
139	Optional Port	Incoming	Distribution Server	Windows Endpoints	This port is required when Windows endpoint uses the NETBIOS protocol. WMI can use NETBIOS over port 139 in case of failure to use port 445 over TCP. If you did not configure the endpoint to use NETBIOS, you do not need to open port 139.
<WMI fixed port>	WMI communications	Incoming	Distribution Server	Windows Endpoints	Configure the endpoint with the WMI fixed port when configuring Active Directory endpoint only.
389	ADSI Communication	Incoming	ENTM	Windows Endpoint	This port is required for managing Windows endpoint
<ADSI fixed port>	ADSI communications		ENTM	Windows Endpoints	Configure the endpoint with the ADSI port.
22	SSH Port	Incoming	ENTM	SSH Endpoint or Network Device	This port is required for managing SSH devices through the SSH protocol.

23	Telnet Port	Incoming	ENTM	SSH Endpoint or Network Device	This port is required for managing SSH devices through the Telnet protocol.
1521	Oracle database port	Incoming	ENTM	Oracle Endpoint	This port is required for managing Oracle endpoints.
1433	Microsoft SQL Server database port	Incoming	ENTM	Microsoft SQL Server Endpoint	This port is required for managing Microsoft SQL Server endpoints.
18080,18443	Optional Port	Incoming	Browser	ENTM	Use this port when using the ENTM web UI from a machine which is behind a firewall.

## ObserveIT Used Ports

ObserveIT uses the following TCP ports:

Number	Description	Listener	Sender	Comments
4884	ObserveIT Agent	ObserveIT Application Server	ObserveIT Agent	By default, the communication is not SSL-enabled. Use port 443 if you enable SSL communication.
4884	ObserveIT Web Console	ObserveIT Application Server	ObserveIT Agent	By default, the communication is not SSL-enabled. Use port 443 if you enable SSL communication.
1433		Database Server	ObserveIT Application Server and ObserveIT Web Console	

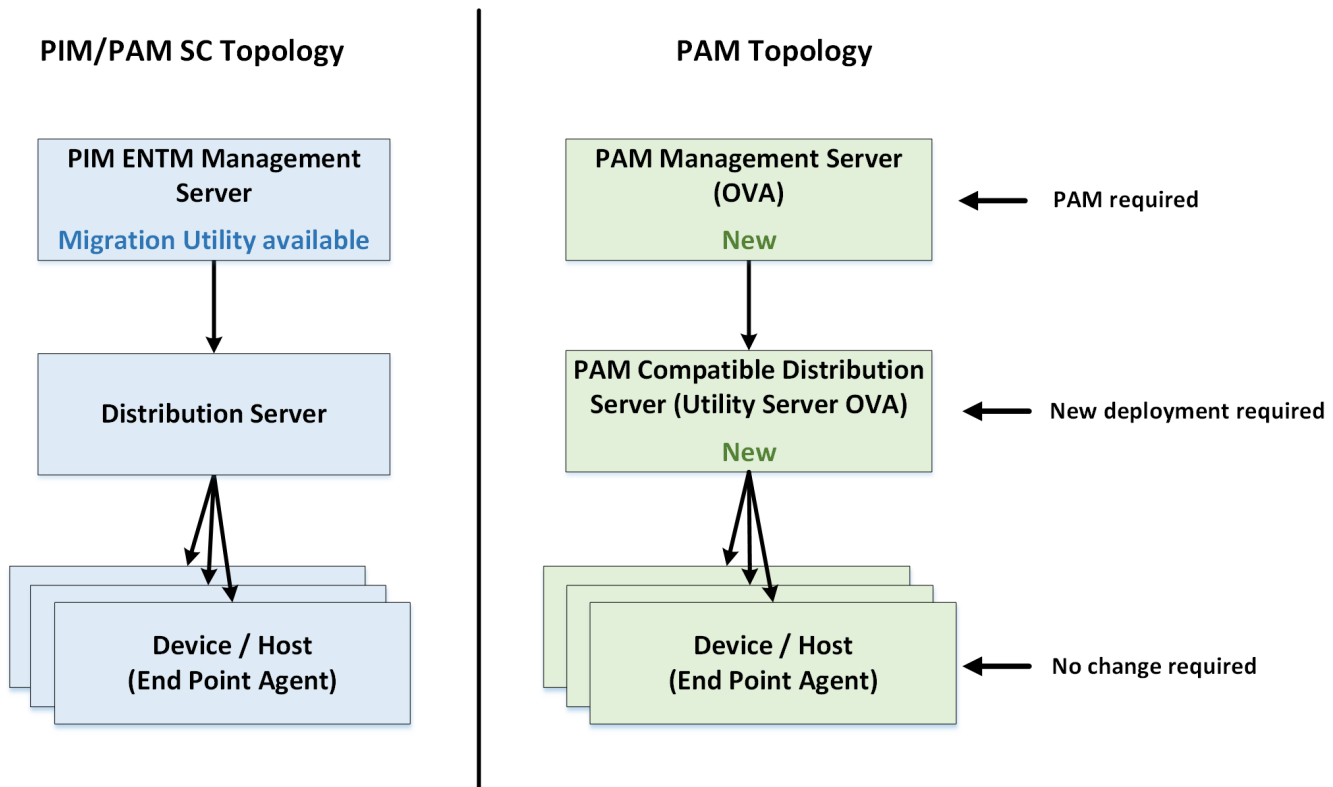
## PAM SC Frequently Asked Questions

This content answers common questions that PIM or PAM SC administrators may have when migrating to PAM:

### **If I use Advanced Policy Management with the ENTM and endpoints, what changes in the new PAM framework?**

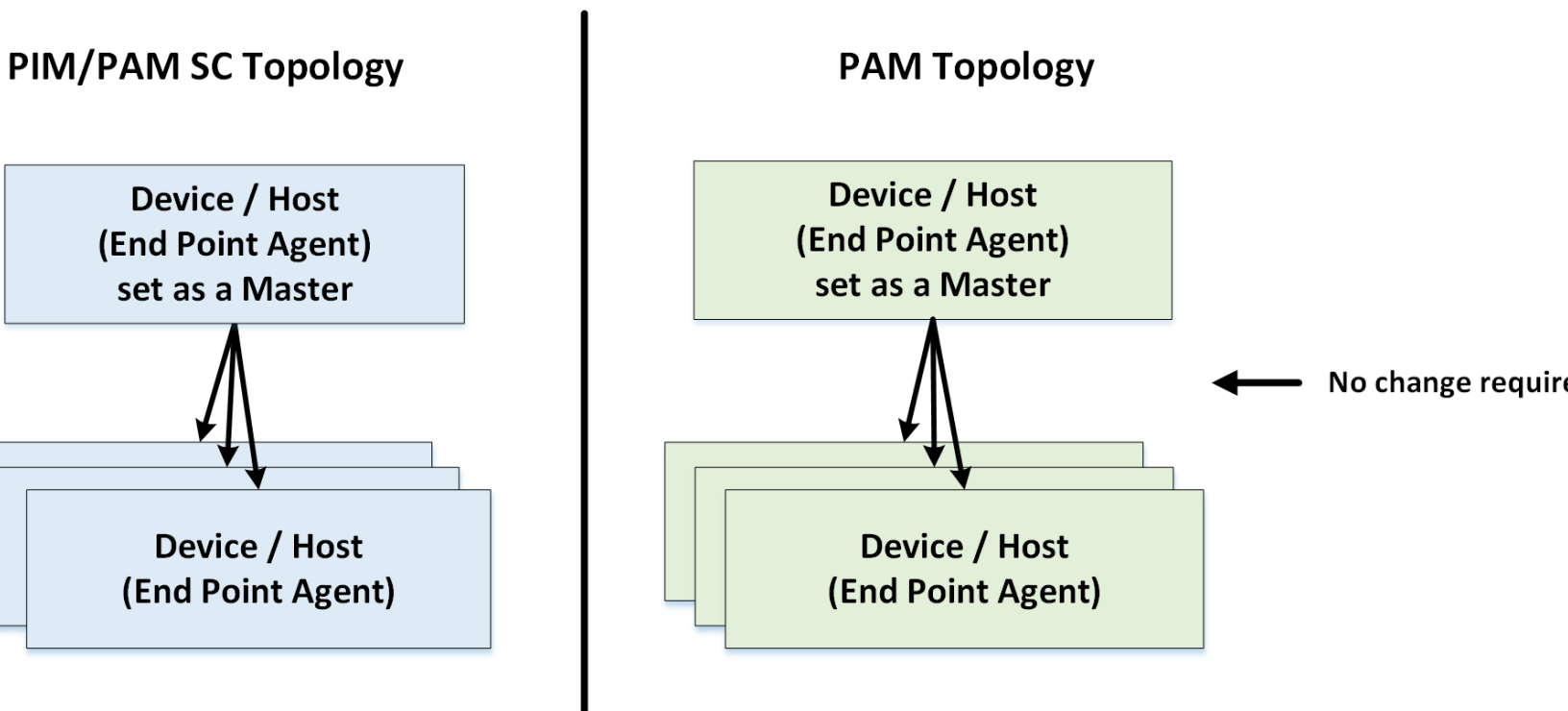
The endpoints remain the same, but ENTM is integrated into the PAM server. The Distribution Server is replaced by the new Utility Appliance.



**Figure 57: Difference between PIM/PAM SC and PAM Advanced Policy Management****If I use PMDB, can I still use endpoints only and assign one of the endpoints as a master to set policies?**

You can continue to use the endpoints as you have been doing with no impact.

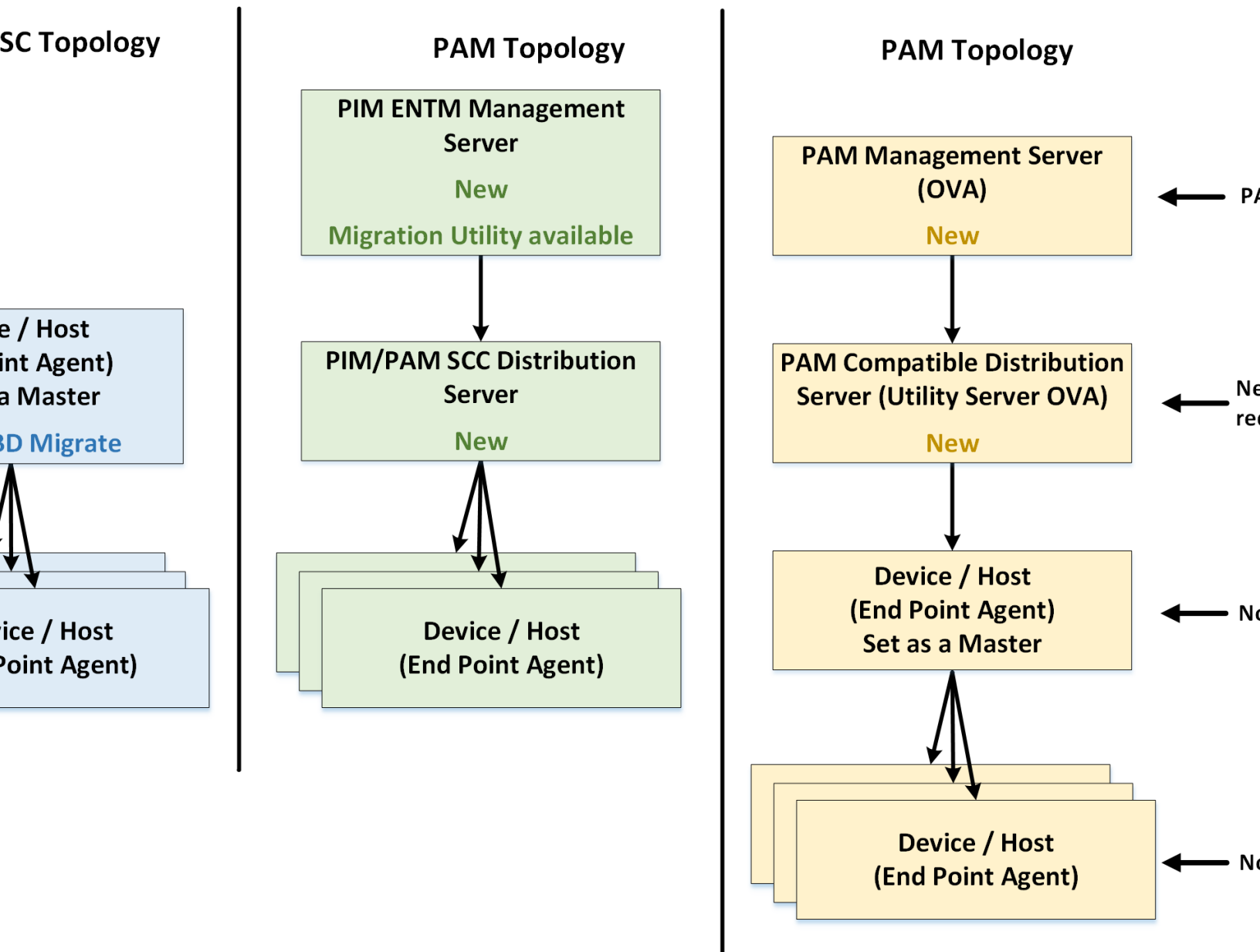
To use Server Control functionality in PAM, you must first upgrade to Advanced Policy Manager with a Distribution Server. Then use the Migration Utility to migrate to PAM 4.0 and the new Utility Appliance.

**Figure 58: Difference between PIM/PAM SC and PAM PMBD**

Another PMBD option is to change the configuration to an Advanced Policy Management setup. To change the configuration, follow two processes:

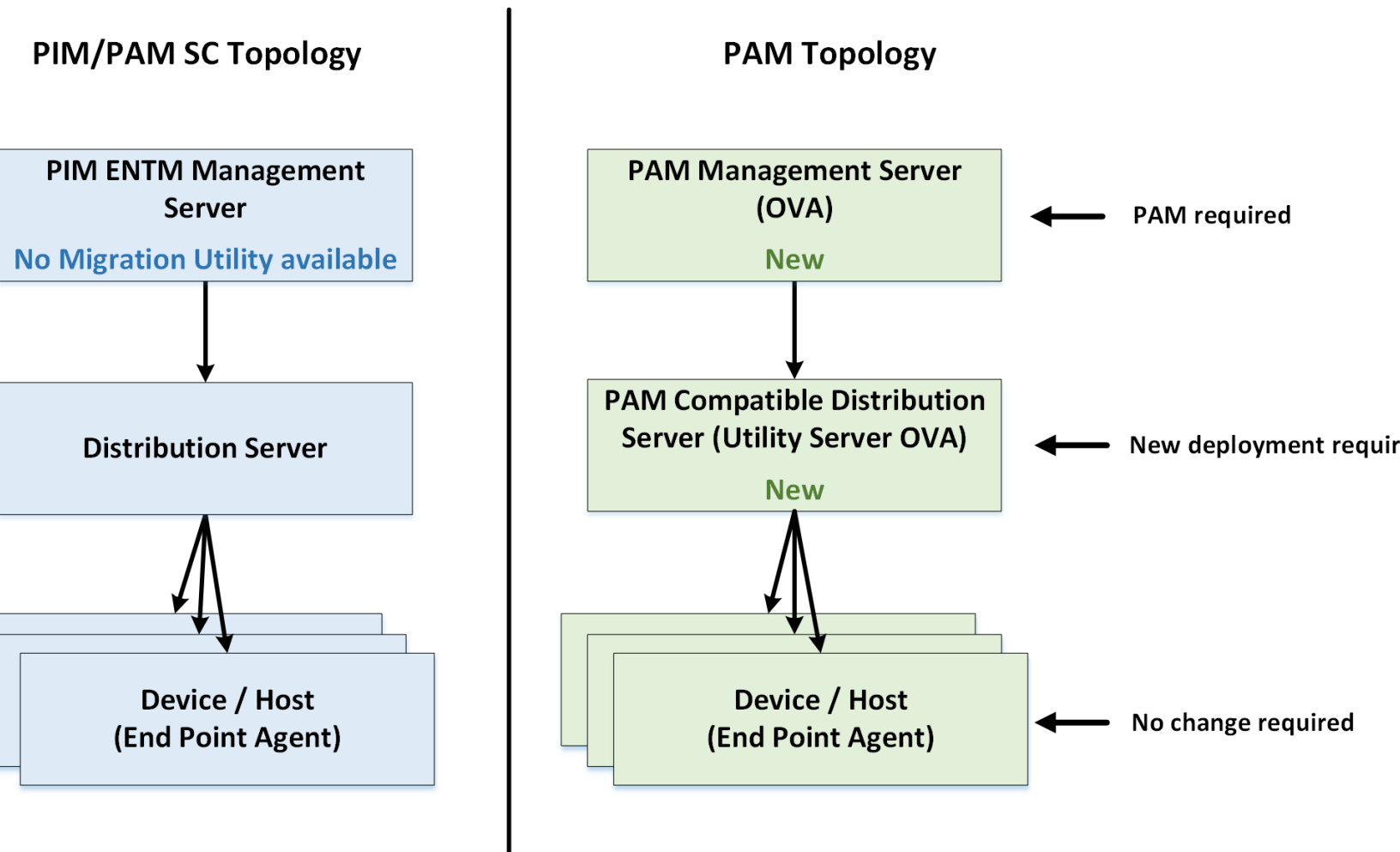
1. Add an ENTM management server plus the distribution server.
2. Migrate to the PAM configuration shown in the following diagram. This option uses the PAM architecture and its benefits.

Figure 59: Migrating to PAM PMBD through PAM Advanced Policy Management

**Is Share Account Management (SAM) supported in PAM 4.0?**

SAM is supported in PAM 4.0. However, PAM 4.0 does not include a utility to migrate SAM information, so the only way to use SAM is to manually migrate all the required data.

Figure 60: Difference between PIM/PAM SC and PAM Share Account Management

**What are the legacy PIM and PAM SC components, and how does PAM fit into PAM 4.0?**

See the following table for information on the legacy PIM and PAM SC components:

**Legacy Components:**

Legacy Component	New Component	Migration Utility Available?
ENTM (Enterprise Manager)	PAM server	Yes
DS (Distribution Server)	Utility Appliance	Yes
PMDB (Policy Model Database)	PAM server & Utility Appliance	Yes
SAM (Shared Account Management)	PAM server	No, manual migration

- **ENTM: Enterprise Manager:** The Enterprise Management Server was the central management server. This server contained components and tools that let you deploy policies to endpoints and define resources, accessors, and access levels. The server also contained components that manage the communication between the Enterprise Management Server, the endpoints, and other components. An embedded Privileged Access Manager Server Control endpoint was silently installed when installing the Enterprise Management Server. The embedded Privileged Access Manager Server Control endpoint protected and supported the applications in the Enterprise Management Server.

The Enterprise Manager is replaced by the PAM 4.0 server.

- **DS: Distribution Server:** The Distribution Server handled communication between the Enterprise Management Server and the endpoints. By default, an embedded Distribution Server was installed on the Enterprise Management Server. The Distribution Server is replaced by the Utility Appliance.
- **PMDB: Policy Model Database (Replaced by PAM server and Utility Appliance):** The PMDB contained users, groups, protected resources, and rules governing access to the resources. In addition, the PMDB contains a list of subscriber databases. Each subscriber is a Privileged Access Manager Server Control database that resides on a separate computer, or another PMDB that resides on the same or another computer. A PMDB that updates a subscriber is the parent of the subscriber.  
The PMDB is replaced by the PAM server and Utility Appliance.
- **SAM: Shared Accounts Management (No Migration Utility - Only Manual Migration):** SAM previously provided role-based access management for privileged accounts on target endpoints from a central location. SAM provided secure storage of privileged accounts and application ID passwords. SAM also controlled access to privileged accounts and passwords that are based on policies you define. Further, SAM managed privileged accounts and application password lifecycle and let you remove passwords from configuration files and scripts.  
Only manual migration is available for SAM.
- **UNAB: Unix Authentication Broker:** The Unix Authentication Broker is used when you want to manage and control access to UNIX hosts through Active Directory users and groups. UNAB lets you log into UNIX hosts using an Active Directory user name and password. Users and groups do not need to be defined on NIS or `/etc/passwd`. Information can be taken from Active directory.  
UNAB does not require Access Control Endpoint in order to operate; it is supplied as a stand-alone installation.

### **Where can I find the new architecture?**

See the [PAM 4.0 Architectural Overview](#).

### **Which virtual deployment platforms and hardware are supported?**

PAM 4.0 supports VMware OVA and physical hardware. Azure, AWS, and Google Cloud are NOT supported in this release.

### **Is ActiveMQ still used by PAM 4.0?**

ActiveMQ is still used, but the list of use cases has changed. Each Utility Appliance runs an ActiveMQ instance, but it is a single standalone component that is in place to support the current endpoint technology stacks.

### **Is Tibco supported in PAM 4.0?**

PAM 4.0 supports Tibco / 12.x agents. TIBCO is not supported by default. For more information, see [TIBCO Configuration in PAM](#).

### **I do not use Enterprise Manager in my deployment today; can I still migrate to PAM?**

If you do not use Enterprise Manager, you can still migrate to PAM 4.0. If you are managing your endpoints and policies from disconnected Distribution Servers, you can install and run the Migration Utility on the Distribution Server. Then extract the data to import into PAM. Repeat this migration on each Utility Appliance.

# Implementing Threat Analytics

---

Threat Analytics is a powerful tool for identifying anomalies in PAM user behavior and implementing policies to dynamically mitigate potential insider threats or breaches by external threat actors. As a PAM administrator, you interact with the Threat Analytics utility using the [Threat Analytics Console](#).

## Threat Analytics Capabilities

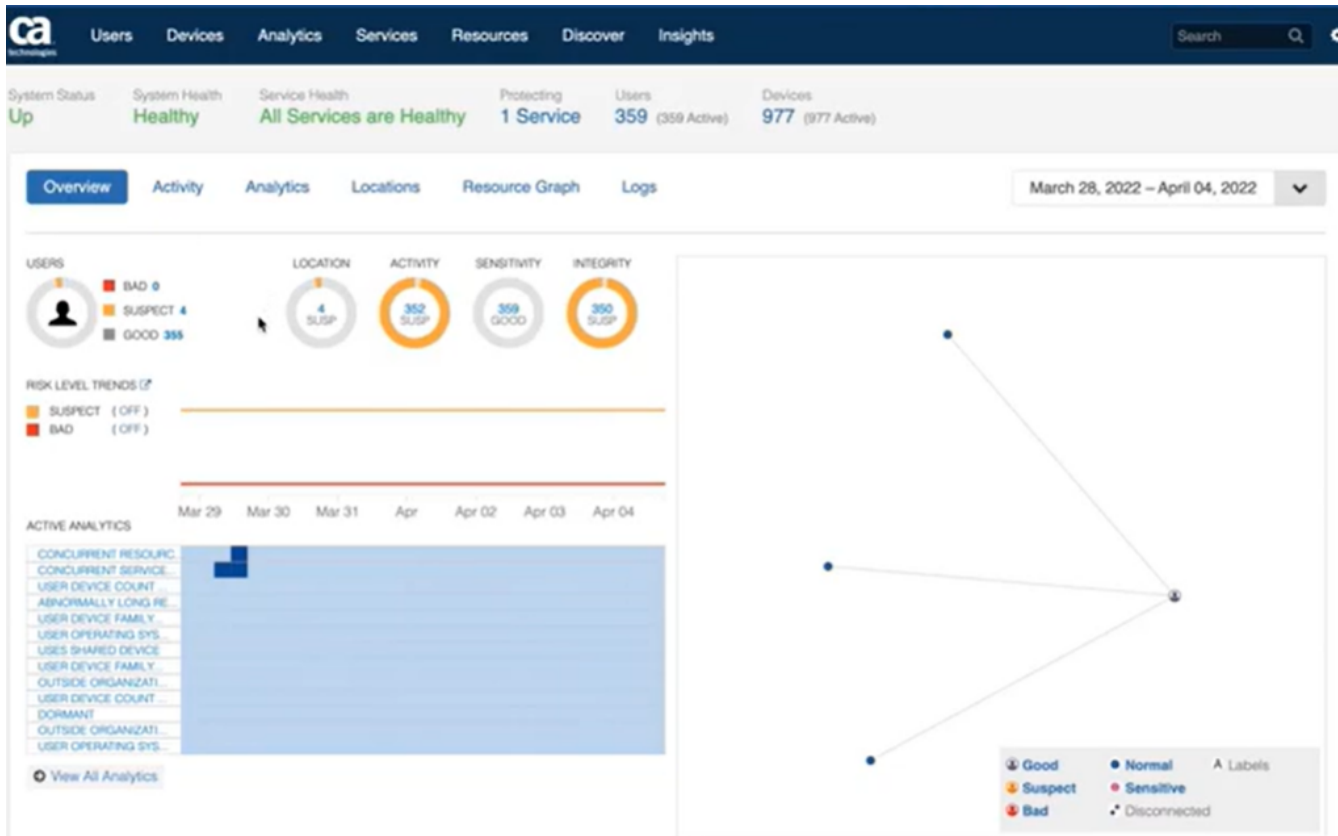
Threat Analytics provides capabilities that enable you to perform the following tasks:

- **Gather information on the threat landscape over time, from past events to the current moment:**
  - Zero in on [specific users](#) and [devices](#).
  - View the [services](#) and [resources](#) being used.
  - Get a [summary of risky activity within a selected time span](#), zeroing in on suspicious events.
- **Set the policies and thresholds that trigger a threat assessment for a user or device:**
  - View in detail all [58 analytics](#) that can be applied; each one can be enabled or disabled as needed.
  - [Modify the parameters](#) used to make risk status decisions.
  - See all [analysis and status decisions](#) that have been made on the PAM network at different slices of time.
- **Interpret, summarize, and filter any and all network activity:**
  - See visual [mapping of potential threats](#) and risky users.
  - [View the Data Insights](#), which includes key summary data for all PAM operations.
- **Identify the threat landscape across an entire organization, from the overall threat snapshot down to the threat assessment for an individual user or device.**
  - Enable or disable users based on their [IP location](#) or [country](#).
  - Configure the logging and reporting (via email notification that is managed by the [STMP protocol](#) and [Syslog/SIEM logging](#)) of all threats that are captured by the console.
  - Export the threat assessment and share it with appropriate audiences.

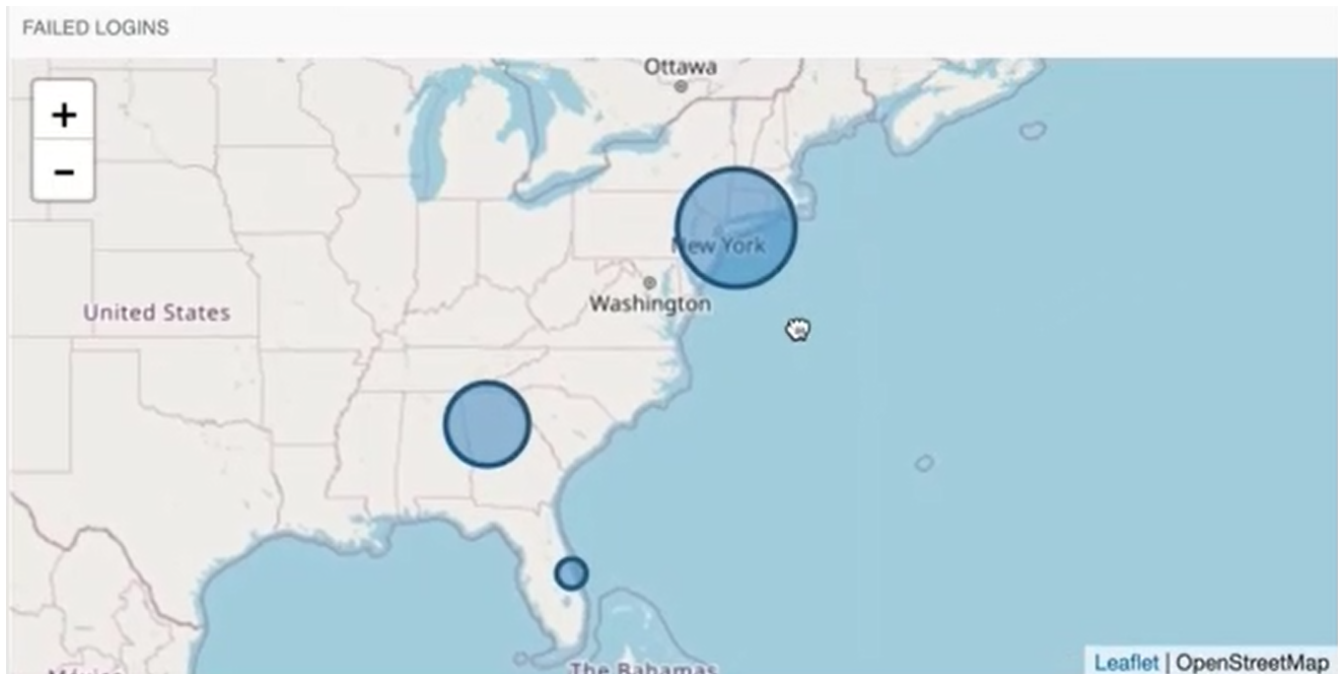
## Threat Analytics Console

You interact with Threat Analytics using the *Threat Analytics Console*. The console provides graphs, maps, and other rich visualizations to help you analyze the threat data, as shown in the following examples:

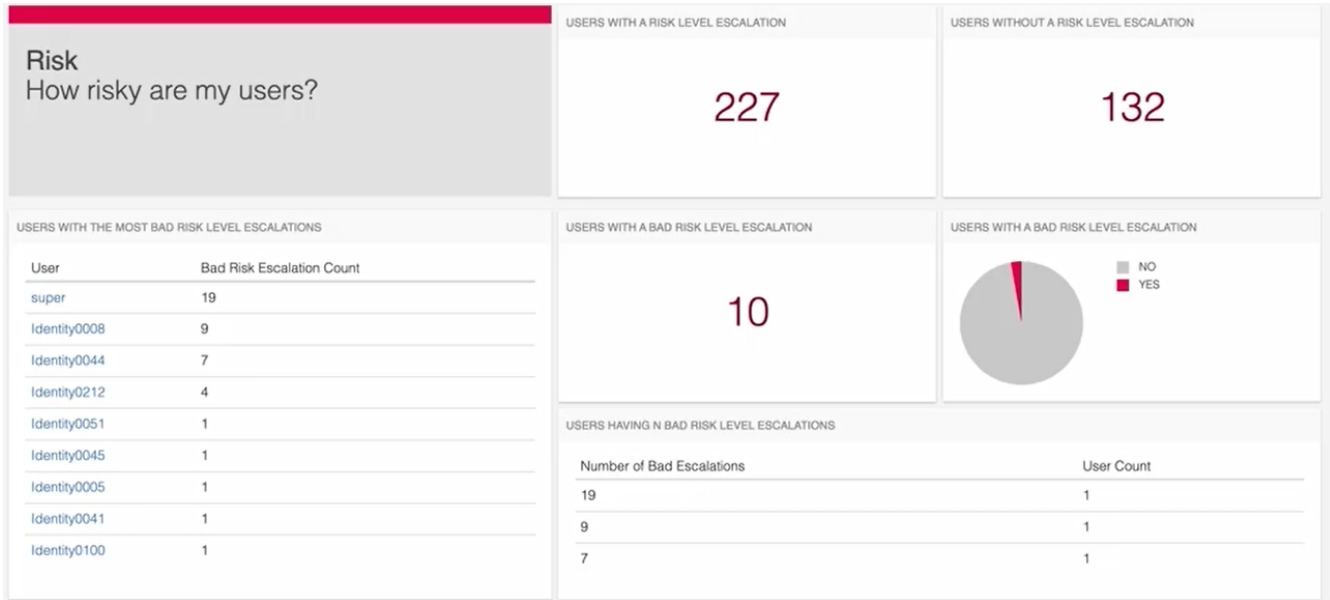
- View user and network threat activity at a glance:



- Use a geolocation view of the PAM network to see clusters of suspect users.



- Risk view shows counts of users with and without new risk level escalations and the number of users with Bad and Suspect risk-level escalations.



## Integrate Threat Analytics

Symantec Threat Analytics integrates with Privileged Access Manager to evaluate the risk of privileged user activity to detect and mitigate threats from suspicious activity. Evaluation factors include the location of a privileged user, time and duration of activity, the system connections, and user history for security.

By persistently monitoring activity, Threat Analytics identifies the anomalies based on historical user behavior. The analytics server returns a risk level to PAM. The risk level can dynamically trigger activities, such as starting session recording or prompting the user to reauthenticate.

The integration of Symantec Threat Analytics and PAM is explained in the following topics:

### Threat Analytics and PAM Server Interaction

The two servers interact following this sequence:

#### 1. **PAM collect event data.**

PAM collects event data and forwards it to the threat analytics server. Events include:

- Logging in and out of the PAM appliance.
- Opening or closing a connection to a target device or endpoint

New event data is forwarded immediately. Entities other than PAM might also forward events for the same users.

#### 2. **Threat Analytics analyzes event data.**

The threat analytics server performs continuous analysis on the collected data. Each existing user has a *risk level* that is assigned one of the following values:

- Good
- Suspect
- Bad

For each new event, the received data is compared against past behavior for that same user. If the data is for a user without a threat server records, Symantec Threat Analytics prepares a new record. The service then begins compiling data for that user.

Based on continuous analysis and the historical data for a user, Symantec Threat Analytics might change the risk level. The server then return the result to Privileged Access Manager. Risk level changes do not always happen immediately after receiving event data; the change might occur later.



### 3. PAM applies mitigations

Depending on the returned risk level or changes to the risk level, PAM can take actions against users. These actions are called *mitigations*.

#### Mitigations Applied Against Threats

The risk level that Symantec Threat Analytics returns determines the actions which PAM takes against the user.

Risk Level	Mitigation
Good	None
Suspect	Session Recording Recording begins for any current connection session until the end of the session. The server records all future connection sessions in their entirety.
Bad	Re-authentication and Session Recording Any current login and device-connection sessions are suspended. PAM forces the user to re-authenticate by displaying a login window.  For all applets, session activity pauses and the applet window disappears. The reauthenticate window then opens. For any TCP service, such as PuTTY or OpenSSH, the terminal window remains open, but you cannot enter anything in it.

#### Session Recording Mitigations When Risk Level Changes

Session recordings span over time. When the user has a connection session in progress that is being recorded, the following rules also apply:

Risk Level	Changes To	Behavior
Good	Suspect or Bad	<ul style="list-style-type: none"> <li>A new recording of that session begins immediately.</li> <li>Recording continues until the end of that session.</li> <li>Subsequent connection sessions are recorded from beginning to end.</li> </ul>
Suspect or Bad	Good	<ul style="list-style-type: none"> <li>Recording continues until the end of that session.</li> <li>Subsequent connection sessions are not recorded, unless an applicable policy specifies session recording.</li> </ul>

#### NOTE

- [Deploy the Symantec Threat Analytics Server](#)
- [Enable Mitigation Actions](#)
- [Set up SAML Punch-Through Authentication \(Optional\)](#)

## Deploy the Symantec Threat Analytics Server

The Symantec Threat Analytics Server is distributed as an OVA virtual machine (VM) image. To integrate Privileged Access Manager with Threat Analytics, deploy the Threat Analytics Server as a VM image on a compatible virtualization environment in your network.

**WARNING**

If PAM is operating in FIPS mode, PAM servers can integrate only with Symantec Threat Analytics version 2.2.3 or later.

Beginning with version 2.2.3, the Symantec Threat Analytics server supports the TLS v1.2 protocol for secure communications. TLS v1.2 is required to work with PAM in FIPS mode.

To integrate PAM with Threat Analytics, complete the following procedures in order.

**Apply the Symantec Threat Analytics License**

Threat Analytics is a separately licensed component of Privileged Access Manager. If you are deploying a new appliance independently or in a cluster, you might already have a Symantec Threat Analytics license. Otherwise, follow these steps, to be done in the PAM UI, to activate Symantec Threat Analytics on your currently installed appliance.

1. Obtain a PAM license file with **Threat Analytics** licensing activated from Broadcom support.
2. Log in to PAM UI as **super**, or an account with an equivalent role such as Global Administrator.
3. Navigate to **Configuration, Licensing**.
4. In the **Install New License** tab, use **Choose File** to browse for the license file.
5. Select the correct file, and then select **Upload License File**.
6. In the pop-up dialog, select **Save New License**.
7. Under **Configuration, Licensing, Current License**, confirm that the "Threat Analytics Capability" item is set to "Enabled."
8. Repeat these steps for each appliance in a cluster.

**Deploy the Symantec Threat Analytics Server VM**

Deploy the Threat Analytics Server virtual machine image on any virtualization environment that supports OVAs.

Complete the following steps to install the server in a virtual environment:

1. [Verify the Virtual Machine Requirements](#)
2. [Download the Symantec Threat Analytics software](#)
3. [Deploy the Threat Analytics VM on the Virtualization Environment](#)
4. [Configure NTP for the system time](#)
5. [Set up networking](#)
6. [Configure the Threat Server SSL Settings](#)

***Verify That the Virtualization Environment Can Support the Threat Analytics VM Requirements***

For a production environment, verify that the virtualization environment can support the following minimum requirements for the Threat Analytics Server VM:

- CPU: Eight cores
- Memory: 16 GB
- Storage: One TB

***Download the Symantec Threat Analytics Software***

Download the software for this component from the Broadcom Support site. For information on how to download it, see [Download PAM Installation Media](#).

***Deploy the Threat Analytics VM on the Virtualization Environment***

Do this procedure to deploy the Threat Analytics VM on your virtualization environment.

**Follow these steps:**

1. Using the import tools available in your virtualization environment, import the Symantec Threat Analytics OVA. Create a virtual machine with at least the minimum production requirements. For more guidance on how to size the virtual machine, contact Broadcom Support.
2. Start the virtual machine.
3. In the VM console window, a blue menu screen is displayed. Click the blue screen and switch to the login screen by pressing the **Ctrl+Alt+F2** keys simultaneously. If that fails to open the Linux console, press **Alt+Fn+F2** simultaneously.
4. Log in to the Linux console.
  - The default login credentials for the 2.4.x version are *interlock/interlock*.
  - The default login credentials for the 2.3.x version are *root/8iyhko6kx*.
5. After first-time login using default credentials, change the password of the system users as follows:
  - For the 2.4.x version, run *sudo bash* to become the root user.
  - Run *passwd interlock* to set the interlock user password.
  - Run *passwd root* to set the root user password.

**NOTE**

SSH access to the Symantec Threat Analytics server is disabled by default. Use the VM console to access the Linux console for SSH access if necessary.

**Configure NTP for the System Time**

Symantec Threat Analytics requires the system time to be set, and is preconfigured to use public NTP. If you do not have access to public NTP servers, use an internal NTP server to enable the time synchronization with the virtualization host.

**Follow these steps to configure NTP for the System Time:**

1. Log in to the Symantec Threat Analytics Linux console as a root user.
2. Type `date -R` to see the current date and time. Use the `-R` to get a standard unambiguous format.
3. Edit the `ntp.conf` file using the following command on a terminal with root privileges:  
 Command to run on 2.4.x: `sudo vi /etc/ntpsec/ntp.conf`  
 Command to run on 2.3.x: `sudo vi /etc/ntp.conf`
4. Add the following line to the configuration file:  
`server <IP_of_NTP_Server> prefer iburst`
5. Restart the NTP service by running the following command on a terminal with root privileges:  
 Command to run on 2.4.x: `sudo systemctl restart ntpsec`  
 Command to run on 2.3.x: `sudo service ntp restart`
6. To check the NTP service, run the following command:  
`sudo ntpq -p`
7. Log out of the VM console by typing **exit** to return to the login prompt.
8. Return to the network configuration screen by pressing the **Ctrl+Alt+F1** keys simultaneously. If that fails to return to the configuration screen, press **Alt+Fn+F1** simultaneously.

**Set up Networking for the VM**

Networking for the VM environment can be set from the main VM console window, with no need to log in.

**IPv6 is supported in Symantec Threat Analytics 2.4.0 onwards. Support for IPv6 is not added to Symantec Threat Analytics 2.3.x versions.**

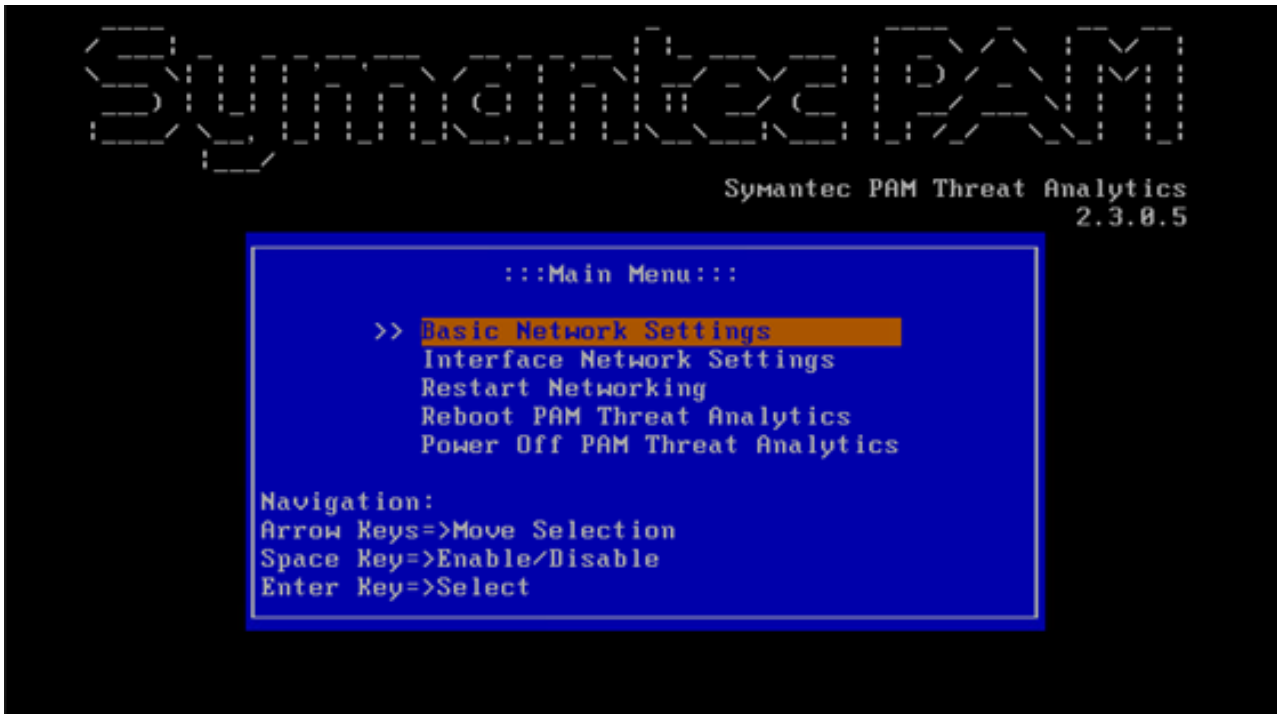
The 2.4.x console UI is shown in the following screen:



Six options are listed on this screen:

- Basic network settings
- IPv4 interface network settings
- IPv6 interface network settings
- Restart networking
- Reboot PAM Threat Analytics
- Power off PAM Threat Analytics

The 2.3.x console UI is shown in the following screen:



Five options are listed on this screen:

- Basic network settings
- IPv4 interface network settings
- Restart networking
- Reboot PAM Threat Analytics
- Power off PAM Threat Analytics

Use the following controls to navigate the menu:

- Use the Arrow keys to move the selection.
- Use the Space key to enable/disable.
- Use the Enter key to select.

### ***Configure the Threat Server SSL Settings***

The Symantec Threat Analytics OVA ships with a default JKS that contains a self-signed certificate. This JKS allows the threat server to work after the initial installation, and it is appropriate for test instances. To be cryptographically secure and trusted in production, replace the default JKS with one containing your own security certificate. If you decide not to use SSL, select the **SSL Validation off** box during the configuration of PAM for Symantec Threat Analytics.

Use one of the following procedures to set up SSL on the Threat Server:

1. [Create a Java Key Store file](#)
2. [Set up SSL settings](#)

### **Create a Java Key Store File**

The Symantec Threat Analytics OVA ships with a default JKS that contains a self-signed certificate. This JKS file allows Symantec Threat Analytics to work upon the initial installation, and is appropriate for test instances. To be cryptographically secure and trusted in production, replace the default JKS with one containing your own security certificate.

**To create a JKS file, follow these example steps:**

The sample commands use the following placeholders:

- **CA**: PEM-encoded issuing certificate authority
  - **crt\_file**: PEM-encoded X.509 signed certificate file; **key\_file**: PEM-encoded X.509 private key file
  - **alias**: An arbitrary name (letters, numbers, dashes)
  - **p12\_file**: Filename for the temporary .p12 file
  - **jks\_file**: Filename for the resulting JKS file
1. Use the **openssl** command to combine the Certificate Authority, the signed certificate, and a private key into a p12 file.
 

```
openssl pkcs12 -export -in <crt_file> -inkey <key_file> -out <p12_file> -name <alias> -CAfile <CA> -caname root
```
  2. Use the **keytool** commands to convert the p12 file into a keystore.
 

```
keytool -importkeystore -destkeystore <jks_file> -srckeystore <p12_file> -srcstoretype PKCS12 -alias <alias>
keytool -import -alias root -keystore <jks_file> -trustcacerts -file <crt_file>
```

**Set up the SSL Settings**

After you generate a new JKS file, set up the SSL configuration.

**Follow these steps:**

1. Access the Symantec Threat Analytics Administration UI. For example: **https://ServerIPaddress:3000**
2. Log in with the user name *admin* and password P@ssword1234.
3. Change the password using the Password tab.
4. Go to the **Security** tab.
5. In the **JKS File** field, select **Choose File** and upload a JKS file. A valid JKS file has an X.509 server certificate and trust chain. For more information, see [Create a Java Key Store File](#).
6. In the **Server Alias** and **JKS Password** fields, enter the appropriate values.
7. Verify that the **SSL Protocols** field is set appropriately. The default values are TLS v1 and TLS v1.2.
 

**NOTE**

If PAM is operating in FIPS mode, TLS v1.2 is required for secure communications. TLS v1.2 is available only with Symantec Threat Analytics version 2.2.3 onwards.
8. Select **Save**.
9. Navigate to the Symantec Threat Analytics Administration home.
10. Restart the Threat Analytics Engine by clicking its **Restart** button.

**Deploy Symantec Threat Analytics in Azure*****Prerequisites***

Privileged Access Manager instance or cluster that is deployed in Azure and licensed for Symantec Threat Analytics.

***Upload Symantec Threat Analytics VHD to a Storage Account***

The following steps assume you have access to a **Storage Account** previously created for storing a Privileged Access Manager VHD as outlined in [Deploy a VHD to Azure](#). If you must create a new **Storage Account**, ensure that its **Resource Group** and **Location** are the same as the **Resource Group** and **Location** containing your Privileged Access Manager instance or the Primary Site of your Privileged Access Manager cluster.

**Follow these steps:**

1. From the Azure Portal, navigate to the **Storage Browser** panel.
2. On the left-hand menu, select the storage bucket from the Storage Browser.

3. Select the **Container** bucket used to store the Privileged Access Manager VHD. If no bucket exists, you can create a new one.
4. In the selected **Blob Containers**, select the folder that you would like to choose and click **Upload**.
5. Under **Files**, select the Symantec Threat Analytics VHD on your local system, and then click the Upload button to upload the VHD to Azure.

### **Create a Managed Disk for Symantec Threat Analytics**

Follow these steps:

1. Enter "disks" in the search field at the top of the Azure Portal.
2. Select **Disks**.
3. On the **Disks** page, select the **+Add** button to add a new Disk.
4. Provide a **Name** for the disk.
5. For **Resource Group**, select "Use Existing," and then select a Resource Group.
6. For **Region**, select the same location as your Storage Account. Create a disk in the same location as the storage account where you uploaded your VHD.
7. For **Account Type**, select "Premium (SSD)."
8. For **Source Type**, select "Storage Blob."
9. In the **Source Blob** field, use the Browse button to select the VHD you uploaded in the previous step. Select the Storage Containers and then VHD. Click **Select**.
10. For **OS**, select Linux.
11. For **VM generation**, select Gen 1.
12. For **Size (GiB)**, enter at least 1024.
13. Select **Create**.

### **Create the Symantec Threat Analytics Virtual Machine**

Follow these steps:

1. On the **Disks** page, select the newly created Symantec Threat Analytics disk.
2. Select **+Create VM**. The **Create Virtual Machine** panel appears.
3. In the **Basics** tab, enter a Name for your VM.
4. For **Resource Group**, select "Use Existing" and select your Resource Group.
5. **Region** is disabled because it is determined by the disk Storage Account Location.
6. Select a machine Size that meets the minimum requirements for Symantec Threat Analytics. See Machine Requirements for more information.
7. Under **Select Inbound Ports**, ensure that only ssh (22) and https (443) are selected.
8. Select the **Networking** tab.
9. For **Virtual Network** and **Subnet**, use the same Virtual Network and Subnet that contains your Privileged Access Manager instance or the Primary Site of your Privileged Access Manager cluster.
10. For **NIC Network Security Group**, select Advanced.
11. Under **Configure Network Security Group**, select **Create New**.
12. Select **Add an inbound Rule**.
13. To access the Symantec Threat Analytics Administration UI, add a rule for **Destination Port** of 3000 with TCP selected for **Protocol**.

#### **NOTE**

Create public IPv6 in Azure "All Services" and select the IPv6 resource in the **Networking** tab. This step is optional.

14. Select **OK** to return to the Network tab.
15. Select the **Tags** tab.

16. Add a new **Tag** with the **Name** "PAMIgnore" and the **Value** of "true." Under **Resources**, ensure that only "Virtual Machine" is selected. This setting prevents PAM from importing the Symantec Threat Analytics VM as a standard target device if the "Sync Virtual Machines" option is enabled for the PAM Azure Connection.
17. Select **Review + Create**.
18. Verify the settings on the **Summary** page and then select **Create** to finish. Deployment begins. To monitor its progress, you can select the **Notifications** bell icon in the upper right.

### **Configure Symantec Threat Analytics**

Configuring Symantec Threat Analytics requires configuration on the PAM appliance and the Symantec Threat Analytics. The final steps to configure Symantec Threat Analytics are to:

1. [Enable the PAM External API](#)
2. [Configure the Threat Engine to use the Adapter](#)
3. [Specify the Symantec Threat Analytics Server to Use](#)
4. [Threat Analytics and Admin Users](#)

#### ***Enable the External API***

Enable Symantec Threat Analytics to communicate with Privileged Access Manager using its API. The account password can be updated and used for the Threat Analytics configuration. **Follow these steps:**

1. In the PAM UI, navigate to **Configuration, Security, Access**.
2. Select **Enable** for the **External REST API** setting.
3. Select **Save**. This message appears: External API Access has been updated successfully.
4. Select **Configuration, Licensing, Current License**. Confirm that the PAM license has "Threat Analytics Capability" set to "Enabled."
5. Select **Credentials, Manage Targets, Accounts**.  
After applying a PAM license that enables Threat Analytics Capability, an API key with an account name of the format CATapApiUser-x (for example, CATapApiUser-2001 ) is created automatically.  
This account contains credentials that are used by Symantec Threat Analytics to complete the configuration. Under the **Action** column, select the **eye** icon to view the password and copy it for later use.
6. The password for this account can be updated by selecting this account and clicking the Update button. This password is used later while configuring the Threat Analytics engine for PAM.

#### ***Configure the Threat Engine to Use the Adapter***

Specify the PAM adapter for the Threat Server on the Symantec Threat Analytics server. **Follow these steps:**

1. From a browser, access the Symantec Threat Analytics engine. For example, `https://threat_server_ip_address`
2. Log in as **admin** with password **P@ssword1234**. (Change this default password!)
3. Navigate to **Services**.
4. Select Privileged Access Manager from the Services list.
5. Select the **Configuration** tab.
6. Specify the values for the following API connection parameters:
  - **Host:** The IP Address or hostname of the PAM instance (Do not include https://)

#### **NOTE**

If PAM is a cluster configuration, then the PAM primary VIP address must be used as the host. If a literal IPv6 address is used to identify the PAM instance, then the literal IPv6 address should be enclosed in square brackets. For example: `[fd6d:8d64:af0c:1::13ad]`



**IPv6 support is added in Symantec Threat Analytics 2.4.x onwards.**

- **Username:** The username of a user with Symantec Threat Analytics API Access (such as CATapApiUser-x ; for example: CATapApiUser-2001 )
  - **Password:** The password of the user with access to the Symantec Threat Analytics API. Use the password that you copied from the CATapApiUser-x Account in PAM.
7. Select **Test** to validate the provided parameters and verify connectivity to PAM.
  8. Once validated, select **Save Configuration**.
  9. While still in Services Privileged Access Manager, select the **Auth Tokens** tab. This step generates the API Auth Token.
  10. Select **New Auth Token**.
  11. In the window, provide a token **Name** and an optional **Description**.
  12. Select **Create Token**.  
A page displays with the generated token and Service Identifier.
  13. Save the token.
  14. Copy or download the token and Service Identifier. You need both to set up the Symantec Threat Analytics server in the PAM UI.
    - To copy the token, copy both strings from the token confirmation window that is displayed after saving it.
    - To download the token to another location, select **Download Token**.
  15. Close the New Auth Token confirmation window.

**Specify the Symantec Threat Analytics Server to Use**

Specify the Symantec Threat Analytics service that receives the user data from PAM for processing. **Follow these steps on each instance:**

1. Log in to the PAM UI and navigate to **Configuration, Symantec Modules, Threat Analytics**.
2. Enter values for the following fields:
  - **Threat Analytics Address:** Enter an IP address or FQDN for the server hosting the service.

**NOTE**

For IPv6 addresses, do not enclose the address in square brackets. For example, fd8d:8d64:af0c:1::

**IPv6 support is added in Symantec Threat Analytics 2.4.x onwards.**

- **Threat Analytics Authentication Token:** Enter the authentication token string that is generated by the Symantec Threat Analytics server. Get this string from the Threat Server administrator. This token is analogous to a password for access to that server.
- **Threat Analytics Service ID:** Enter the service identifier string that is generated by the Symantec Threat Analytics server. Get this string from the Threat Server administrator. This identifier is analogous to a username for the server.

**NOTE**

A Threat Analytics Server administrator can find the Authentication Token and Service Identifier in the downloaded Token file.

- Optionally, to turn **SSL Validation off**, select this checkbox.
3. Select **Save**.
  4. Test the validity of the connection by selecting **Test**. Wait for a configuration message that the connection is successful.

**Threat Analytics and Admin Users**

Licensing Threat Analytics creates the TAP Administrators group (Threat Analytic for PAM Administrators Group).

**NOTE**

If you already have a User group named "TAP Administrators" in your environment, delete it or rename it to avoid a duplicate group name violation error.

All new or existing users with either the Global Administrator or the Operational Administrator role are automatically added to this group. Similarly, users that lose these roles are automatically removed from this group. Removing the Threat Analytics license deletes the TAP/Threat Analytics for PAM Group. This group cannot otherwise be modified or deleted. The TAP policy gets created with this TAP group and TAP device.

**NOTE****Next Steps:**

- [Enable Mitigation Actions](#)
- [Set up SAML Punch-Through Authentication \(Optional\)](#)

## Enable Threat Analytics Mitigation Actions

Enable mitigations to configure Privileged Access Manager to act in response to the risk level returned by the Symantec Threat Analytics server. For more information about mitigation actions, see [Integrate with Symantec Threat Analytics](#).

### Enable Mitigations

To enable mitigations, follow these steps:

1. From the Privileged Access Manager UI, navigate to **Settings, Global Settings**.
2. Select the **Threat Analytics** tab.
3. Set the **Enable Mitigations** option.
4. Select the **Save** button at the bottom of the pane to activate mitigation actions, effective immediately.

### *Display a Warning Message*

Optionally, display a message near the top of their landing page when a user logs in warning them that data about their activities is being collected.

Follow these steps:

1. Navigate to **Settings, Global Settings**.
2. Select the **Threat Analytics** tab.
3. Set the **Show Analytics Warning** option.  
Optionally, enter a custom warning message in the text field that appears or accept the default message.
4. Select the **Save** button at the bottom of the pane to activate warning messages, effective immediately.

### Risk Level Color Indicators for Session Recordings

To identify sessions that are indicated as a risk, PAM uses color indicators for the session recording entries.

Privileged Access Manager starts session recording in response to a Suspect or Bad risk level assessment. Each recording entry is marked with a color-coded dot (.) in the Risk column. This indicator identifies the threat level at the time recording was activated.

**NOTE**

These indicators only apply when Symantec Threat Analytics is enabled. No color indicators are applied when the relevant user-device policy specifies session recording.

The following table lists the color indicator for the risk level of a new recording. All entries are for a user with a connection session to a target device. The user is already being recorded and the risk level changed.

Changed Risk Level	Color Indicator	Notes
Good to Suspect	Yellow dot	Indicator remains following completion of the recording, even when the risk level changes back from Suspect to Good.
Good to Bad	Red dot	Indicator remains following completion of the recording, even when the risk threat level changes from Bad to Suspect or to Good.
Suspect to Bad	Yellow dot (Red only if Bad level remains)	The ongoing recording is uninterrupted, and the recording entry remains marked with a yellow dot. This indicator remains even when the level changes back from Bad to Suspect or to Good.  If the threat level remains Bad at the time a new recording is started, that recording is marked with a red square.

In general, when the risk level is elevated as a session recording starts, the applicable indicator is applied to that recording entry.

### Filter Recordings

You can filter the Session Recordings page to display only those recordings that are triggered following an increase in the risk level. You can also filter by timestamp and violation tags.

#### Follow these steps:

1. Navigate to **Sessions, Session Recordings**.
2. Select in the **Search** field. A drop-down panel appears.
3. Apply one or more filters to restrict the list of entries:
  - **Date and Time:** Enter a date or time in one or both of the **From** and **To** fields. Enter the value as formatted in the recordings list. Use a full date-time specification. For example: 2016-10-26 15:01:36 GMT +0300 or a portion of that string that can be interpreted starting from the left, such as:
    - Date and time only: 2016-10-26 15:01:36
    - Date only: 2016-10-26
  - **Socket or command filter violations:** Restrict the list to only socket or command filter violations. Select the **Contains violation** filter to display only those entries.
  - **Risk level.** Restrict the list to a specific risk level. Select one or more risk levels to see only those entries. To select more than one value, hold down the Ctrl key and select each option.

To remove a filter, select the corresponding **Clear** link.

## Set up SAML Authentication (Optional)

To allow authorized Privileged Access Manager users to authenticate seamlessly to the Threat Analytics server, set up SAML-based authentication on the server. This seamless authentication is known as *punch-through authentication*. SAML authentication is optional, but it is a convenient way to connect to the threat analytics server.

**NOTE**

After you configure SAML authentication, you can still log in to the Threat Analytics UI as the local admin user. Keep the admin user account. If the SAML integration fails, you might need to access the Threat Analytics UI as the admin user. To log in as the admin user, navigate to [https:// server\\_ip\\_address/users/sign\\_in](https://server_ip_address/users/sign_in).

To set up SAML authentication between the appliance and the Symantec Threat Analytics UI, complete these tasks:

**Enable the Appliance SAML IdP Configuration**

**Follow these steps to enable the IdP:**

1. In the UI, select **Configuration, Security, SAML**.
2. On the SAML page, select **IdP Configuration**.
3. Select the **Enable IdP** button.  
A message appears indicating that the system is rebooting. You are returned to the log in screen.
4. Log in again and return to the IdP Configuration page.
5. Set the **Entity ID**. The Entity ID must be an HTTPS URL that identifies this appliance instance. This ID is included in assertions that the IdP generates to identify itself. The ID is also included in the metadata file. Example: <https://idp.forwardinc.com>.
6. Specify the **Fully Qualified Hostname**. Specify the Privileged Access Manager domain without the protocol prefix. For example: [idp.forwardinc.com](https://idp.forwardinc.com)
7. Select the **Signature Algorithm**.
8. Select the **IdP Certificate** from the drop-down list.  
If PAM is operating in FIPS mode, use your own FIPS-compliant certificate. Do not use the default certificate that is provided with PAM.
9. After the fields are complete, select **Update IdP Configuration**.  
An update confirmation message appears.
10. Select **Download IdP Metadata** and save the XML metadata file.

**Configure SAML Authentication on the Symantec Threat Analytics Server**

**On the Symantec Threat Analytics server, follow these steps to configure SAML authentication:**

1. Launch the Symantec Threat Analytics Administrative Application. For example: [https://server\\_ip\\_address:3000](https://server_ip_address:3000)
2. Log in with the username "admin" with the default password "P@ssword1234."
3. Change the default admin password on the **Password** tab.
4. Navigate to the **Security** page.
5. In the lower half of the page, complete the following fields:
  - **Authentication Mode:** SAML
  - **SAML Metadata File:** Select Browse and locate the metadata file from Privileged Access Manager. For example: [idp-metadata.xml](#)
  - **Domain name or IP address or TAP server:** Enter the fully qualified domain name or IP address of the Symantec Threat Analytics server.

**Authentication Mode**

**SAML Metadata File**

**Domain name or IP address of TAP server**

6. Select **Save**.  
The content of the IdP metadata file appears in the fields. Select the status of the services. Ensure that you see **active** next to the services before continuing. You might need to refresh the page.
7. Select the Threat Analytics Administration next to the CA logo to return to the main page of the application.
8. Restart the following Symantec Threat Analytics services *in the following order*:
  - PostgreSQL Database
  - Threat Analytics Engine
 Each service has a **Restart** button.

### Access the Threat Analytics Server

After you configure SAML punch-through authentication and SAML authentication at the Threat Analytics Server, you can access the server through the UI.

#### **Follow these steps:**

1. Access the appliance UI. Note the following requirements when you access the appliance:
  - If you access the appliance from a web browser, the URL must contain the same value as the **Fully Qualified Hostname** setting in the IdP configuration. For example, if the Fully Qualified Hostname value is **idp.forwardinc.local**, the URL must be **https://idp.forwardinc.local/cspm/home**.
  - If you access the appliance from the CA PAM Client, on the Client login page, set the **Address** field to **idp.forwardinc.local**.
2. Log in to the UI. Inspect the **Dashboard Overview Tab** that now includes a **Threat Analytics** icon located at the center/bottom of the dashboard.
3. Select this icon to connect to the Symantec Threat Analytics server. Successful access to the server verifies that users can authenticate to the server.

## Configure Threat Analytics Using the Admin Dashboard

This content describes how to configure required Threat Analytics configuration settings using the Threat Analytics Admin Dashboard.

### Log in to the Threat Analytics Admin Dashboard

To login to the Threat Analytics Admin Dashboard, follow these steps:

1. Log in to the Privileged Access Manager UI using an account with Threat Analytics administration privileges.

2. Select the **Access** link on the menu bar to open the **Access** pane, which should include Threat Analytics-related entries as shown in the following screen capture:

Symantec Privileged Access Manager

First name Last Name System Info Logout

Dashboard Access Sessions Users Services Devices Credentials Policies Secrets Settings Configuration

Warning: PAM-CMN-1018: Configuration Password is still the default value.

Devices

Column: Value: Filter Reset Add Filter My Views

Restart Session

Device Name	Address	Operatin	Access Methods	Web Portal	RDP Applications	Services	Target Applications
TAP	10.17.40.160	Other		TAP Admin Dashboard			
tap.ca.com	10.17.40.160	Other		TAP-SAML-Service			

3. Select the **TAP Admin Dashboard** button.
4. When prompted, log in as "admin" using the Threat Analytics administrator password. (The default is "P@ssword1234," which is only intended for the first-time access).

#### NOTE

After initially logging in using the default password, immediately create a new password, as described in [Changing the Admin Password](#).

5. Select the **Sign In** button.

The **Current Status** pane opens, providing the following information:

- The status of the Threat Analytics engine
- The Threat Analytics Admin application
- The Postgre SQL database
- Restart buttons for all three functions if needed.
- All current system information, which is grouped by the following statistics:
  - Current system information, describing the number of cores installed, the current load, and three load averages
  - Current memory statistics, including the total size, how much is being used and how much is available
  - The size of the actual free and shared space in the system
  - The buffer and cache sizes
  - How many Threat Analytics services are running and how much CPU and memory that they are consuming
  - A summary of current disk usage

### Change the Admin Password

To change the Threat Analytics Dashboard password, use the **Password** menu on the **Current Status** pane.

#### IMPORTANT

Change the default password ("P@ssword1234"), immediately after you use it to log in to the dashboard for the first time.

#### Follow these steps:

1. Log in to the PAM UI using an administrator account with the required privileges.
2. Navigate to Configuration, Diagnostics, **Diagnostics Logs**.
3. Enter a new password in the **New Password** field.
4. Enter the new password again in the **New Password Confirmation** field.
5. Select the **Save** button.

### **Upload PAM Analytics Log Files**

By default, Threat Analytics must read all the analytic data from PAM to obtain the previous history of the network. This task must only be done once when Threat Analytics is initially deployed. Loading this data is not required, since Threat Analytics can acquire this data from PAM on its own. However, adding this step dramatically increases how fast Threat Analytics completes its initial "learning" of the PAM environment.

**To obtain the analytics log from the PAM server, follow these steps:**

1. Log in to the PAM UI using an administrator account with the required privileges.
2. Navigate to **Configuration, Diagnostics, Diagnostics Logs**. The **Diagnostic Logs** pane opens.
3. Select the **Download** tab.
4. Select the **Download** button beside the **Analytics Logs** entry.
5. On the **Save** dialog that opens, specify a download directory for the `analytics.logs` file and select the **Save** button.

**To upload the analytics log file into Threat Analytics, follow these steps:**

1. From the Threat Analytics Admin Dashboard **Current Status** pane, select the **Reference Data** menu.
2. Select the **Choose File** button and then locate and select the `analytics.logs` file that you downloaded from PAM.
3. Select **Save**.

The analytics log file is uploaded.

### **Execute Custom Task Files**

If requested to do so by Broadcom Support, you can execute custom task files on the Threat Analytics SQL databases.

**To execute custom threat analytics tasks on the Threat Analytics SQL data base, follow these steps:**

1. From the Threat Analytics Admin Dashboard **Current Status** pane, select the **Tasks** menu.
2. Enter the name of the task that you want to run in the **Tasks** text block.
3. Select the **Run** icon.

The task is executed.

### **Set Up the Security Environment**

To upload Threat Analytics SSL security certificates that are stored in a Java Key Store (JKS) file, use the **Security** menu. On the top section of the pane, you can browse to a JKS file, select it, and then provide your service alias and the key store password. After you select **Save**, you will see detailed information about the security of your network.

**To access information about the security of your PAM network, follow these steps:**

1. From the Threat Analytics Admin Dashboard **Current Status** pane, select the **Security** menu on the Status pane
2. Select the **Browse** button and select the name of the JKS file.
3. Enter the name of the Java Key Store file in the **JKS File** field.
4. Provide the **Server Alias** name (typically "admin").
5. Enter the password for the JKS in the **JKS Password** field.
6. Select the **Save** button.

The following key characteristics of the security environment are displayed:

- **Authentication Mode:** Typically Security Assertion Markup Language (SAML)
- **Assertion Consumer Service URL:** For example, `https://pamtap22.forwardinc.ca/users/saml/auth`.
- **Identity Provider SSO (Single Sign-On) Target URL:** For example, `https://pam34.forwardinc.ca/idp/profile/SAML2/Redirect/SSO`.
- **Identity Provider Entity ID:** For example, `https://pamtap34.forwardinc.ca`.
- **Identity Provider Certificate Fingerprint :** For example, `bfa95c8a41354b1i43ae6bed0d7853a6774bc1`.
- **Assertion Customer Service Binding :** For example, `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`.
- **Identity Provider Certificate:** Approximately 25 lines of alpha-numeric characters.
- **Issuer:** For example, `https://pamtap22.forwardinc.ca`.
- **Compress Request?:** Yes or No.
- **Sign Authentication Requests?:** Yes or No.

To clear the fields in the security pane so that new information (JKS, alias, etc.) can be entered, select the **Reset** button. This step essentially deletes the current configuration if you click **Reset** and then saves it.

To verify the existing security setup so that the connection between PAM and TAP is verified, select the **Test Connection** button. If the customer is seeing errors in their environment, knowing that the connection is successful and verified greatly reduces troubleshooting time.

### **Set Up a Database Backup Schedule**

To set up where and when to save your remote backups and to restore backup data, use the **Backups** menu. In three sections, you can specify daily the **Backup Destination**, specify the **Backup Schedule**, and perform **Restore Backup** operations.

**To set up and restore backups, follow these steps:**

1. At the top right of the screen, select the **Create a New Backup** button.
2. In the **Backup Destination** section, select the **Enable remote backups?** checkbox and enter a Secure Copy Protocol (SCP) user name.
3. Enter the private key in the **Private Key** text box.
4. Enter the hostname of the target server in the **Target Server** field and the path of the target directory.
5. Select the **Set Destination** button at the right.
6. In the **Backup Schedule** section, enter the time of each day's backup and select the **Reschedule** button.
7. In the **Restore Backup** section, select the **Browse** button and choose the files that you want to restore. Then select the **Restore** button.

In the section at the bottom of the **Backups** menu, you see the date and time of the last restore operation. Following that entry is a list of compressed backup files and their creation date, time, and size, each with their own set of **Download**, **Delete**, and **Restore** buttons.

### **Sign Out from the Settings Menus**

To return to the sign-in page, select the **Sign Out** menu. Then select the **TAP-SAML-Service** button from the **Access** menu and you return to the main PAM display, from which you can open the Threat Analytics Console (described in [Launching the Threat Analytics Console](#)).

### **Enable Admin Privileges for Users**

To provide Threat Analytics administration privileges to other existing users, use the **Access** pane. This example enables an existing user named "super."



**Follow these steps:**

1. Select the **Access** menu from the PAM menu bar at the top left of the screen. This menu offers the choice of going to the Admin Dashboard or going directly to the Threat Analysis Console.
2. Switch from **TAP-SAML-Service** to the **TAP Admin Dashboard**.
3. Log in as "admin" using the administrator password. (The default is P@ssword1234).
4. Select the gear icon in the top right of the window and then select **Settings**.
5. Under the **User Accounts** menu tab, find the "super" user that is generated from the SAML logins from PAM, as shown in the following table:

[+ Add User](#)

Login	Email	Admin	Enabled	Locked	Source	Last Login Time	Last Login IP	Actions
admin	admin@localhost.local	✓	✓		interlock	Jul 1, 2022 11:14 AM	127.0.0.1	<a href="#">Edit</a> <a href="#">Delete</a>
sg912053	sam.grant@broadcom.com	✓	✓		interlock	No Logins	N/A	<a href="#">Edit</a> <a href="#">Delete</a>
super	super@pam.local	✓	✓		saml	Jul 5, 2022 7:33 PM	127.0.0.1	<a href="#">Edit</a>

6. In the "Actions" column of the table, select the **Edit** button for the user you want to have admin privileges.
7. On the **Edit User** page, select the "Enabled" and the "Admin" buttons, specify the priority of the **System Alerts**, **Service Alerts**, and **Risk Escalation Alerts**, and then select **Save**.
8. Log back into Admin Dashboard and change the authentication back from **TAP Admin Dashboard** to **TAP-SAML-Service**.

**Launch the Threat Analytics Console**

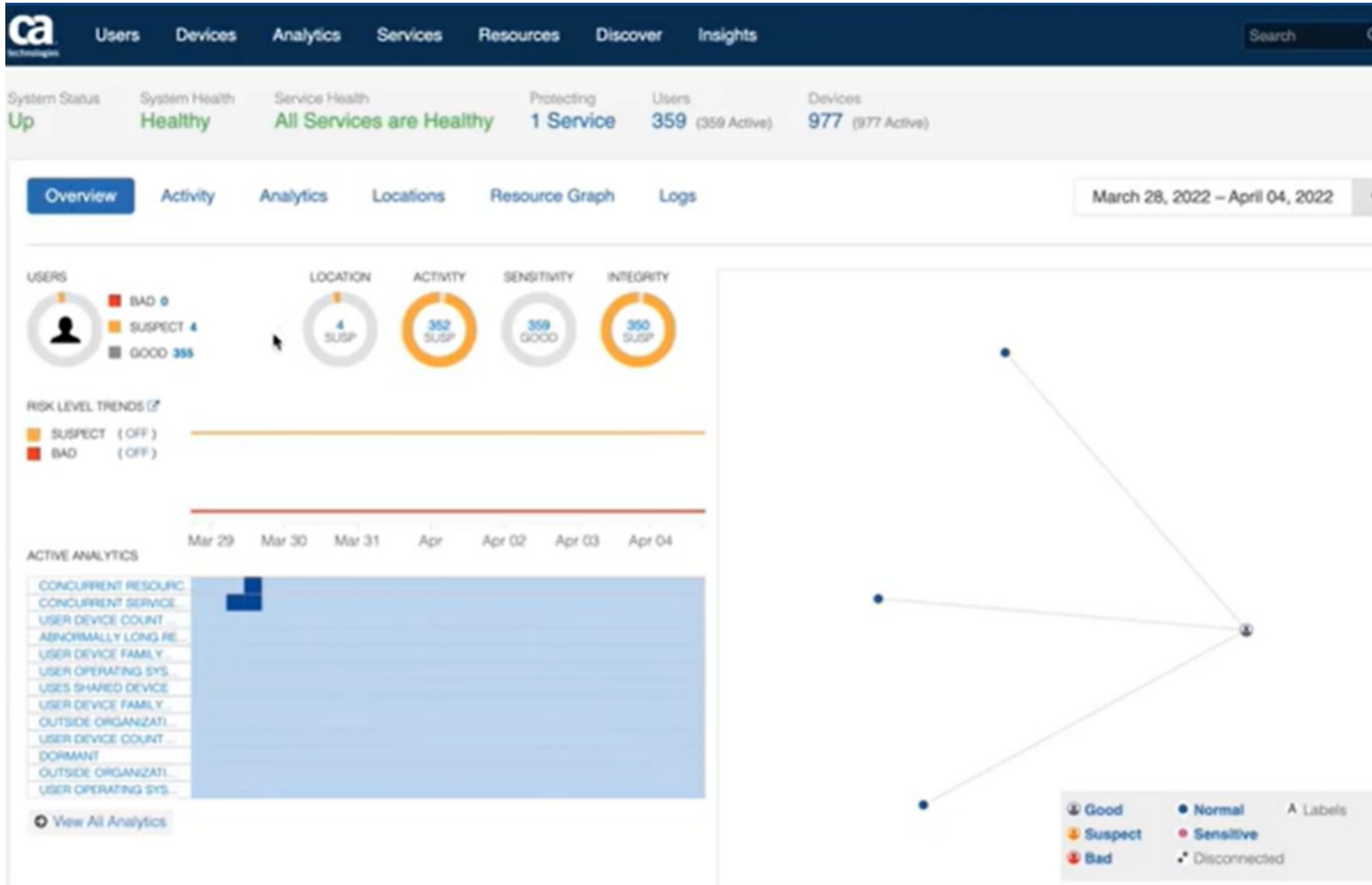
To launch the Threat Analytics Console, open the PAM UI and select the **Threat Analytics** button that is located at the bottom center of the PAM **Dashboard** panel located on the **Dashboard Overview Tab**.

**Analyze User Activity and Analytics**

The Threat Analytics Console opens with a set of six "Home" tabs that provide a big-picture view of the network threats that are encountered over a range of dates you can set (**Overview**), information about activity that is detected on the network (**Activity**), a list of analytics that have been triggered (**Analytics**), the locations of all users (**Locations**), a map of network resources (**Resource Graph**), and detailed logs of network traffic (**Logs**).

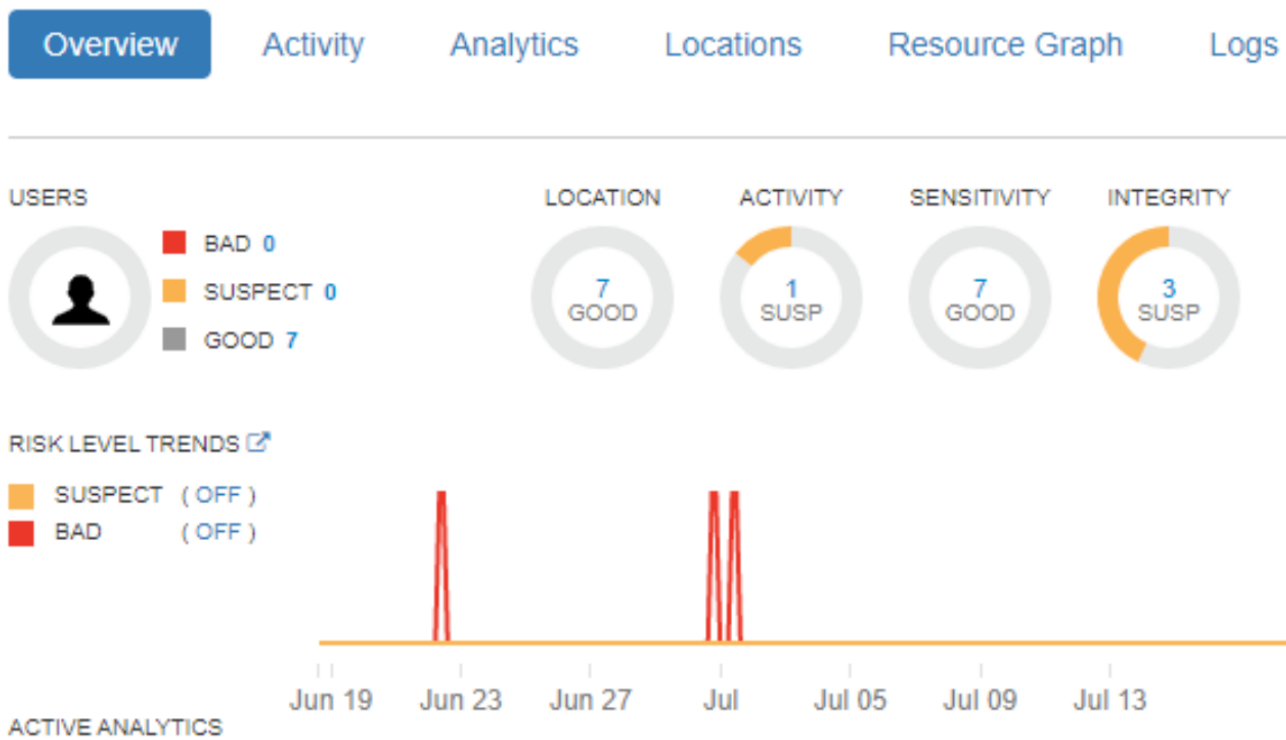
**View User and Network Threat Activity at a Glance**

The Threat Analytics Console appears with the **Overview** tab. This window presents a summary of network activity that is detected over a time period. This range of dates can be specified in the upper-right corner. You can set the start and end dates for the time to analyze, going back to the time you first installed PAM.



## Users and Security Classes

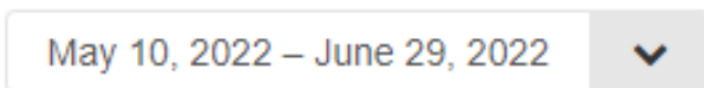
The total number of users in the PAM network appears in the top-left section of the **Overview** window. They are divided into three security categories: **Bad** (in red), **Suspect** (in yellow-orange), and **Good** (in gray). The four circles to the right of the **Users** icon represent how many users have triggered one of four different classifications of the 58 analytics: **Location**, **Activity**, **Sensitivity**, and **Integrity**. The classification of the analytics is described in detail in [Monitor Risk Analytics](#).



Select the blue numbers in each circle to see a list of all individual users that fall into each category. The red and yellow-orange bar graph below them highlights trends and incidents of possible threat activity over the selected time period. The preceding example shows a user with more associated devices than is typical, raising the status of the user to **Bad**. When that particular session ends, the status of the user returns to **Suspect**.

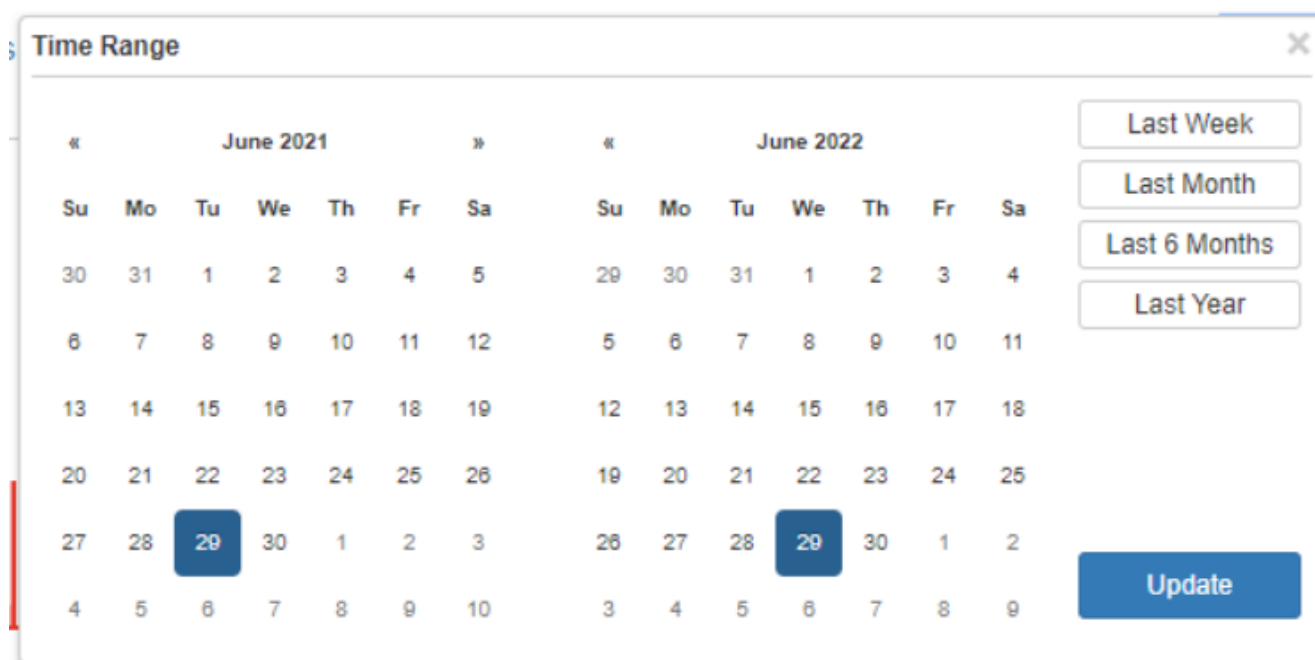
### Active Analytics and the Heat Map

The **Heat Map** on the **Overview** tab provides a list of analytics that were triggered over the designated time period that is specified at the top right of the screen.

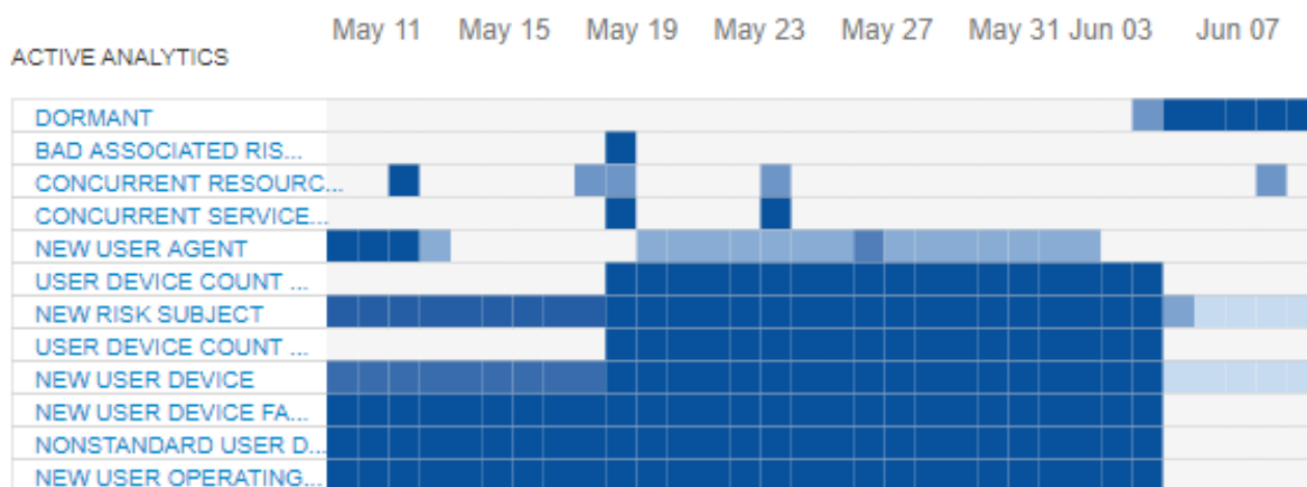


When you select the down arrow, a **Time Range** panel that is similar to a calendar shows the starting year, month, and day and the ending year, month, and day of the desired range.

**Figure 61:**



In the heat map, the level of activity for each detected analytic in the time range is rendered as a bar graph. The activities include all four categories of analytics: **Location**, **Activity**, **Sensitivity**, and **Integrity**. The darker blue blocks show more frequent occurrences of the triggered analytic, the lighter shades of blue show fewer occurrences, and the white color means no occurrences on those days. Undetected analytics do not appear in the **Heat Map**. The example heat map shows 12 analytics that are detected over four weeks. Some analytics in the list are relatively minor, such as new users, new devices, and new device families. But others, such as “Bad Associated Risk Subject,” “Concurrent Resource Sessions,” “User Device Count—Population Limit,” and “New Risk Subject” could indicate potentially dangerous activity.

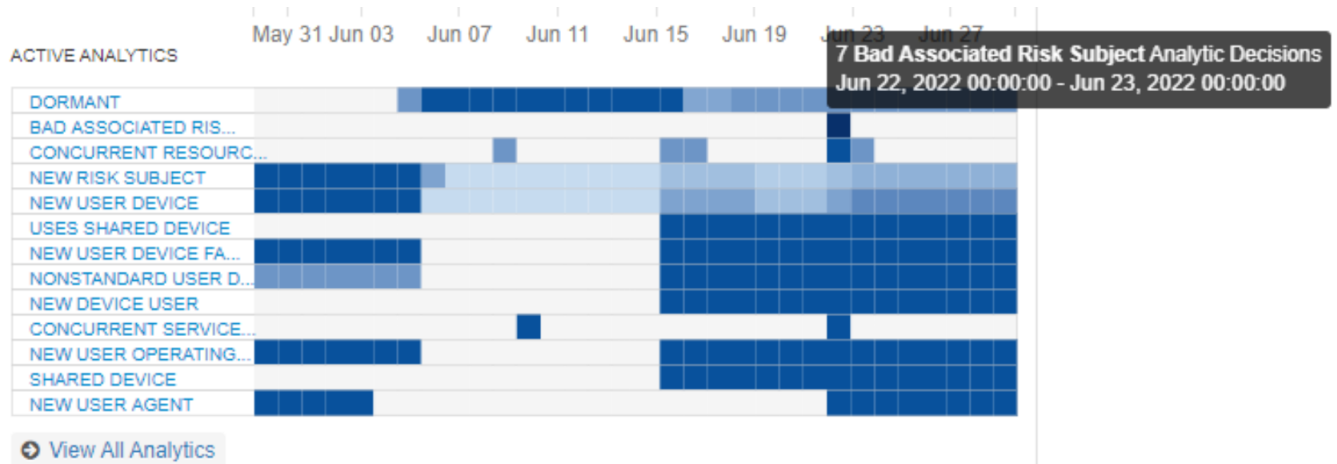


From the blue Active Analytics column on the left, you can select a particular analytic in the heat map to view each instance detected on the time line. The following example shows a list of five different devices that were “Associated with a Bad User” in a single day.

**Bad Associated Risk Subject Analytic Active Between Jun 22, 2022 12:00 AM - Jun 23, 2022 12:00 AM**

Object	Description	Time
e4ad405c1ee6e0a4e880885de4a6... Device	<b>Associated with a bad User</b> Device - e4ad405c1ee6e0a4e880885de4a60bbab26c3c7f76a11426deb3967d93db162b is associated with a bad User - super	7 days Jun 22,
ae21e73862178c4d3a191afc4837a... Device	<b>Associated with a bad User</b> Device - ae21e73862178c4d3a191afc4837af1be2e92594a4011f38389156baa5003d99 is associated with a bad User - super	7 days Jun 22,
6d9dd9cfb3018209ef7bc85ed9155... Device	<b>Associated with a bad User</b> Device - 6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 is associated with a bad User - super	7 days Jun 22,
890ea5626a08013db22b69f89836c... Device	<b>Associated with a bad User</b> Device - 890ea5626a08013db22b69f89836cfeefeb16289fd7fa1ea9c29122ad1830b62 is associated with a bad User - super	7 days Jun 22,
239e1ab7a0c1488e649055c96b9c5... Device	<b>Associated with a bad User</b> Device - 239e1ab7a0c1488e649055c96b9c5c3fb6e7ad99ff1b1e18d83a246c3abde311 is associated with a bad User - super	7 days Jun 22,

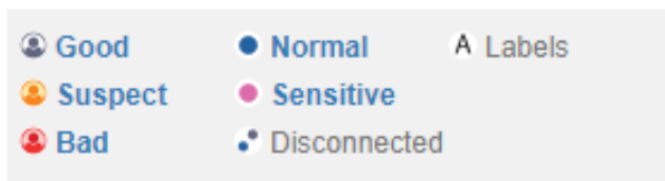
You can also select the colored bars of each analytic in the **Heat Map** on the specific date and time to see all the analytics that were triggered that day.



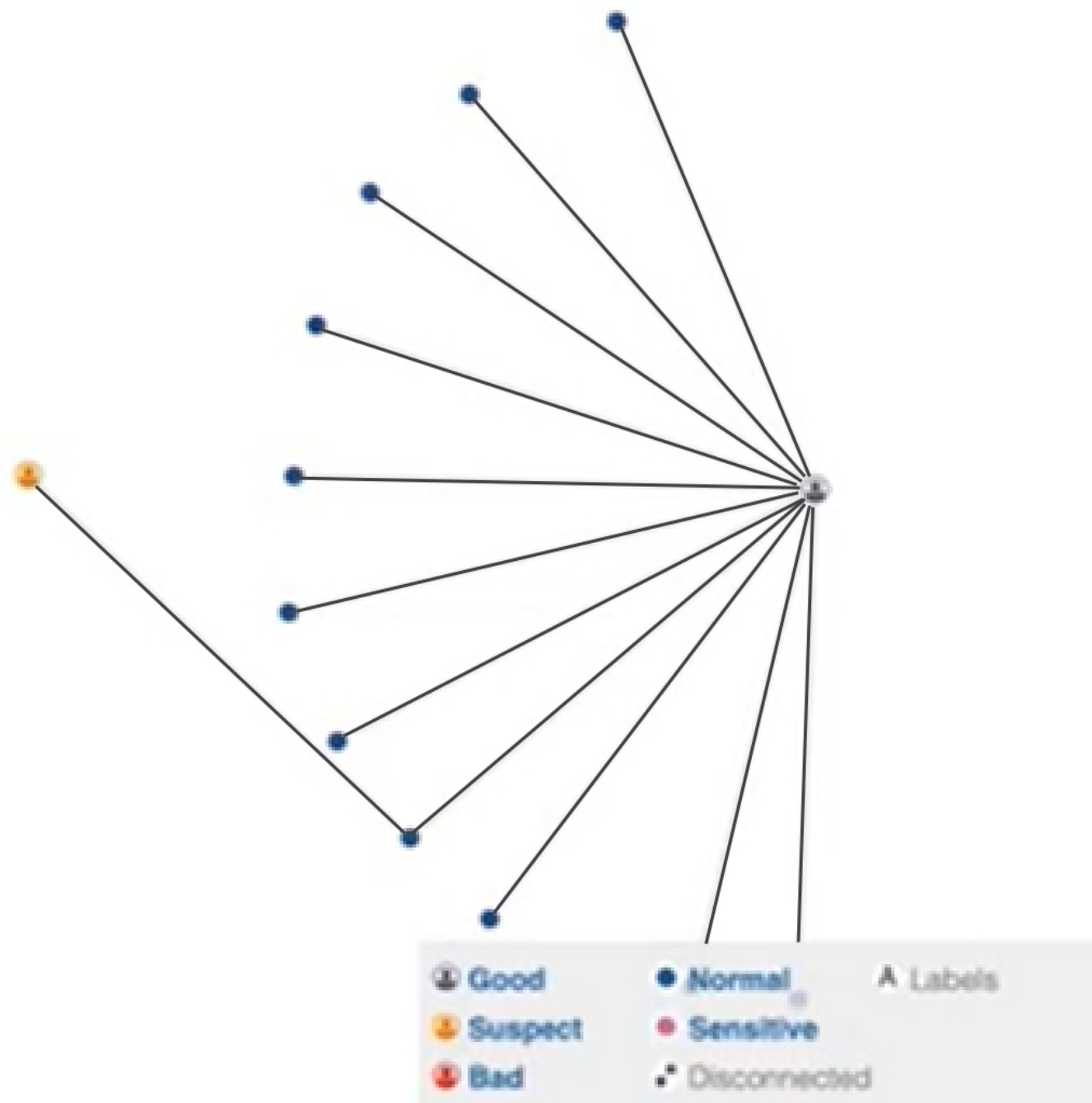
Selecting specific analytics and dates in the heat map timeline can quickly isolate the exact moment when an analytic was triggered and why.

## Network Topology

The **Overview** tab includes a graph on the right pane that depicts the topology of the currently active PAM network, with head-and-shoulder silhouettes colored black (**Good**), yellow-orange (**Suspect**), and red (**Bad**). **Sensitive** and **Normal** users are designated by magenta and blue solid dots, respectively, and disconnected users are shown as a blue and a black dot.



The following example depicts a new **Suspect** user (in yellow-orange) who has accessed the network through one of the **Normal** users.



You can select any icon to get a **User Quick View** that displays the following information:

- The user name
- The date and time of last analytically detected
- The latest IP address of the user
- All the devices used

**User Quick View**

**super**

○ → ● Triggered: Jul 1, 2022 5:31 PM

🌐 Latest IP Address 10.76.13.123

**USER DEVICES (ALL)**

- 📱 e4ad405c1ee6e0a4e880885de4a...
- 📱 ae21e73862178c4d3a191afc4837...
- 📱 6d9dd9cfb3018209ef7bc85ed915...
- 📱 890ea5626a08013db22b69f89836...
- 📱 239e1ab7a0c1488e649055c96b9...

In addition to the **Overview** tab, the **Home** page has five other tabs that provide more detail about the network history over the specified time:

- **Activity:** Examine All Network Activity in Detail
- **Analytics:** Monitor Risk Analytics
- **Locations:** Map User Locations
- **Resource Graph:** Graph Network Resources
- **Logs:** Review Session Logs

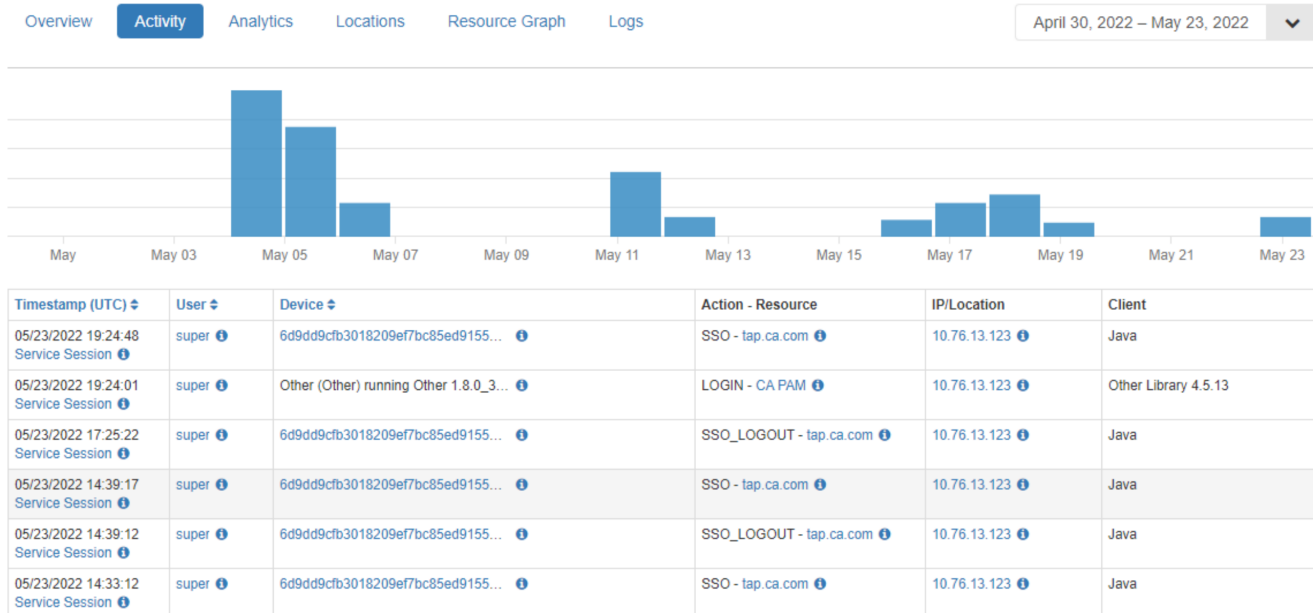
**ca technologies** Users Devices Analytics Services Resources Discover Insights

System Status <b>Up</b>	System Health <b>Healthy</b>	Service Health <b>All Services are Healthy</b>	Protecting <b>1 Service</b>	Users <b>5</b> (5 Active)	Devices <b>6</b> (6 Active)
----------------------------	---------------------------------	---------------------------------------------------	--------------------------------	------------------------------	--------------------------------

**Overview** Activity Analytics Locations Resource Graph Logs

## Examine All Network Activity in Detail

The **Activity** tab opens a list of network PAM sessions during the time period that is specified at the upper right, and also presents a bar graph that shows when and where those particular activities have been detected.

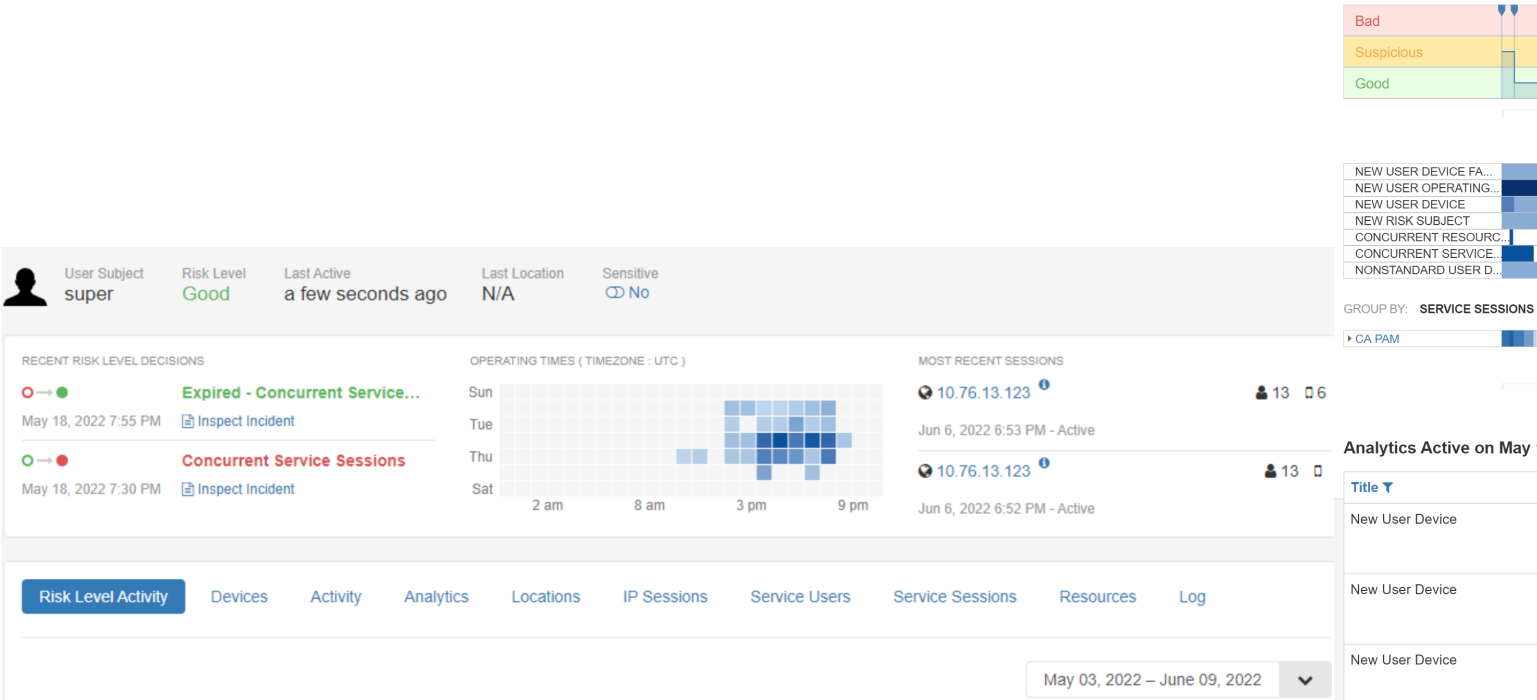


The **Activity** tab lists all activity in the PAM environment, providing the following attributes:

- **Timestamp:** the Coordinated Universal Time code (UTC) for the session
- **User:** the Privileged Access Manager user name
- **Device:** the identity of the system used to log in to PAM
- **Action – Resource:** the action performed (for example, LOGIN or LOGOUT) and the PAM resource used
- **IP/Location:** the IP or location that is used for the activity
- **Client:** the software that allows PAM to establish connectivity with services running on servers.

You can double-click on any user, device, resource, or location on the activity list and can view the **Risk Level Activity** tab, which displays the analytics that are detected over a specific time period. It is similar to the **Overview** pane but adds a top-of-the-screen “header” for the particular user, device, or resource. This area includes some basic status indicators and provides the most recent analytic decision, in this case “Concurrent Service Sessions.” This panel also provides a miniature heat map for the current week and the IP addresses used.





The lower part of the **Risk Level Activity** pane includes the same heat map and table of analytics that were detected over a specified period of time, but it adds a bar graph that shows when this user or device that is changed from **Good** to **Suspicious** or from **Suspicious** to **Bad**, and then back again. This example shows the risk activity for a user who began running concurrent service sessions (displayed in red) and then logged out of the concurrent session. This action then changed the status of the analytic from red back to green. The “Inspect incident” link under the name of each analytic provides a fuller explanation of what was detected.

This heat map also adds an extra separate heat map for the service used (in this case, CA Privileged Access Manager) over the specified time period. The **Risk Level Activity** screens are fully described in [Track Risk Level Activity for All Users and Devices](#).

## Monitor Risk Analytics

The **Analytics** tab provides a list of risk factors that were triggered during the selected period of time, and their associated users or devices. Brief descriptions of the analytics are also provided, along with timestamps.

Overview

Activity

Analytics

Locations

Resource Graph

Logs

June 19, 2022 – July 19, 2022

Title	Object	Description	Timestamp	Annotate
Concurrent Resource Sessions	super User	Concurrent active Resource Sessions detected User - super has more than one active Resource Session initiated from Service - CA PAM	8 days ago Jul 11, 2022 7:55 PM	Annotate
Concurrent Resource Sessions	super User	Concurrent active Resource Sessions detected User - super has more than one active Resource Session initiated from Service - CA PAM	8 days ago Jul 11, 2022 2:54 PM	Annotate
Concurrent Resource Sessions	super User	Concurrent active Resource Sessions detected User - super has more than one active Resource Session initiated from Service - CA PAM	14 days ago Jul 5, 2022 8:34 PM	Annotate
Concurrent Resource Sessions	super User	Concurrent active Resource Sessions detected User - super has more than one active Resource Session initiated from Service - CA PAM	14 days ago Jul 5, 2022 7:55 PM	Annotate
New User Agent	f178399b88384d74a36b3f4690818f... Device	New User Agent Detected Device - f178399b88384d74a36b3f4690818fdd05085e9657711a1233e928e03849fd7f accessed a resource with a new User Agent - Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36.	18 days ago Jul 1, 2022 11:55 AM	Annotate
Concurrent Service Sessions	super User	Concurrent active Service Sessions detected User - super has more than one active Service Session against Service - CA PAM	18 days ago Jul 1, 2022 11:31 AM	Annotate
Bad Associated Risk Subject	6d9dd9cfb3018209ef7bc85ed9155... Device	Associated with a bad User Device - 6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 is associated with a bad User - super	18 days ago Jul 1, 2022 11:31 AM	Annotate

In the previous list, for example, the user was running concurrent resource and service sessions and was also accessing a device associated with a **Bad** user.

If you select the user name, you see a full list of all the analytics that have been detected in that account user in the **Risk Level Activity** pane, and also a timeline and heat map showing when and how often the analytics were detected over time. If you select a device in the **Object** column of the main **Analytics** table, you can see an assessment of **Risk Level Activity** for devices that have questionable status.

The **Annotate** buttons in the right-most column of this table provide the security team with an opportunity to contact a potentially suspicious user and investigate why that incident occurred. If the triggered analytic was unintentional, the team can report that the error was benign in the box labeled “**Was this analytic triggered in Error?**” If needed, a button at the lower right can disable the particular analytic for the user.

Devices

Analytics

Services

Resources

Discover

Insights

## Annotate Concurrent Resource Sessions Analytic

Analytic Title	User	Analytic Expired	Expired At	Timestamp
Concurrent Resource Sessions	super	Expired	May 11, 2022 5:56 PM	May 11, 2022 5:55 PM

Concurrent active Resource Sessions detected  
User - super has more than one active Resource Session initiated from Service - CA PAM

**Was this analytic triggered in Error?**

User reported that in logging on he had very slow network access and mistakenly opened another session.

Update

☒ Concurrent Resource Sessions is enabled for this User  
 Disable this analytic from triggering for this User in the future.

Disable Analytic

The entire set of 58 analytics is included in the default Threat Analytics Console. Users can also go to the admin console to disable some analytics, modify others, or create analytics as needed. The analytics fall into four categories: **Location**, **Activity**, **Sensitivity**, and **Integrity**

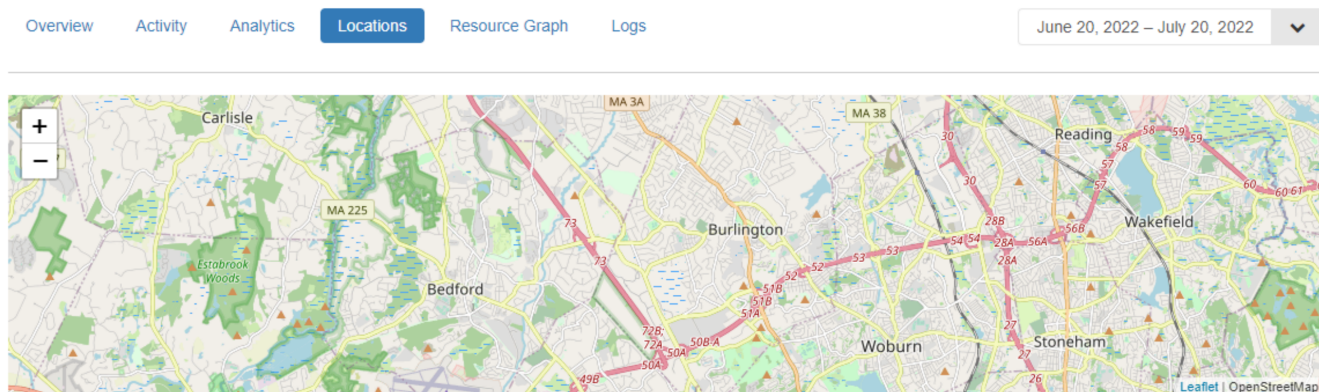
- There are 12 **Location** analytics that are based on the locations of the user or devices. These flag events such as the usage of blacklisted locations, changes of country, and unusual distances traveled. Users operating outside their normal location or outside the location of their organization can also be flagged. So can “impossible” transfers in which a user changes locations at speeds and distances that are implausible or unlikely.
- There are 17 **Activity** analytics that are triggered by potentially risky behavior. Some examples are abnormal resource session rates, overlong service sessions, and access denials. Others are concurrent resources or service sessions, and excessive data downloads. Analytics can detect multiple active VPN “tunnels,” overlong times, and the lack of activity for a preset time period that automatically turns “active” users into “dormant” ones.
- There are four **Sensitivity** analytics that detect access of a sensitive resource or user and that check for excessive group counts over a preconfigured hard limit or statistical/population-based limits.
- There are 25 **Integrity** analytics that flag the appearance of deactivated users or “bad” risk subjects, new users, new devices or shared devices, operating systems, risk subjects, user agents, device families, or outside subnets. They also warn of suspicious users, clients or IP addresses, and excessive network population and device families. An excessive number of operating systems in use or suspicious users and clients are also flagged. Not all of these conditions are necessarily dangerous (such as a new user or device), but they provide protection against a broad range of potential integrity threats.

Based on the triggering of these 58 analytics, the Threat Analytics Console can make decisions about when the behavior of a **Normal** user's has become **Suspect** (or “suspicious”). The console flags certain activities and users with the yellow-orange color in the dashboard and forces PAM to start a recording of that session. These preventative measures begin regardless of how the user set up the access policy. Threat Analytics then continues to monitor that user for all subsequent sessions, devices, and resources accessed to determine whether the risk level of a user must be further escalated.

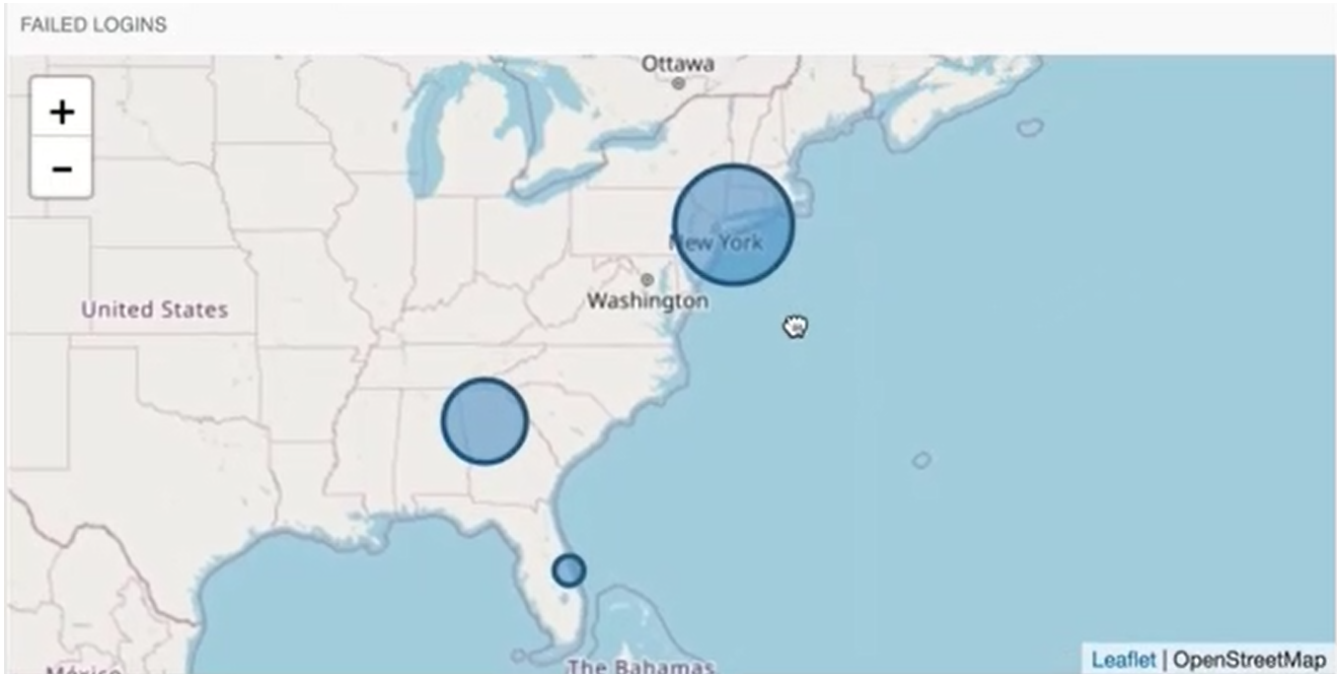
If so, the user goes from **Suspect** to **Bad** and the Threat Analytics Console then locks every session. The console then makes that user reauthenticate with name, password, and (optionally) a multi-factor sign-in to prove who they say they are. If they cannot, it terminates the session. This policy can, for example, help suppress someone who was able to intercept a one-time password to get into that initial session. If this user were to begin doing things that a normal user wouldn't do, the console can recognize the activity and require another set of authentications.

## Map User Locations

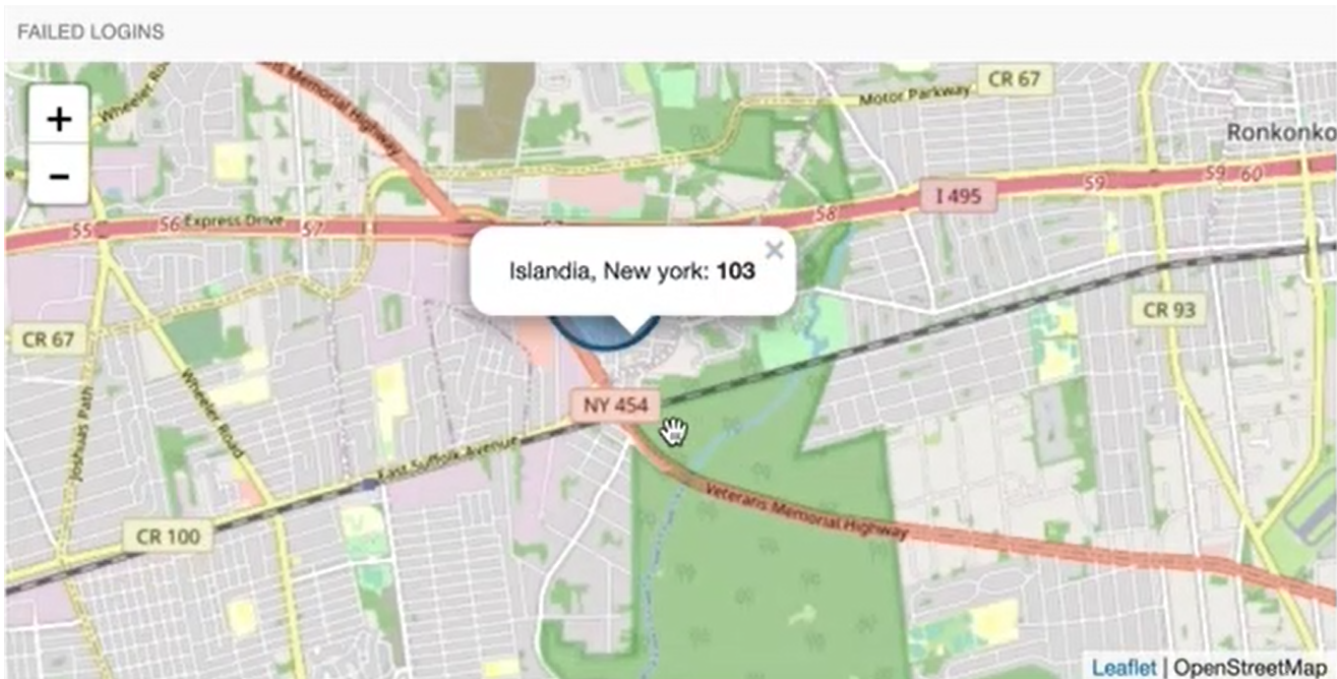
The **Locations** tab on the **Home** page provides a geolocation view of the PAM network that is based on IP addresses.



In the example below, you can see clusters of suspect users in Florida and Georgia, but the largest number of users are from Islandia, New York.



You can select locations on the map to get a closer view of suspect user locations going all the way down to the street-level detail. This one is a view of Islandia:



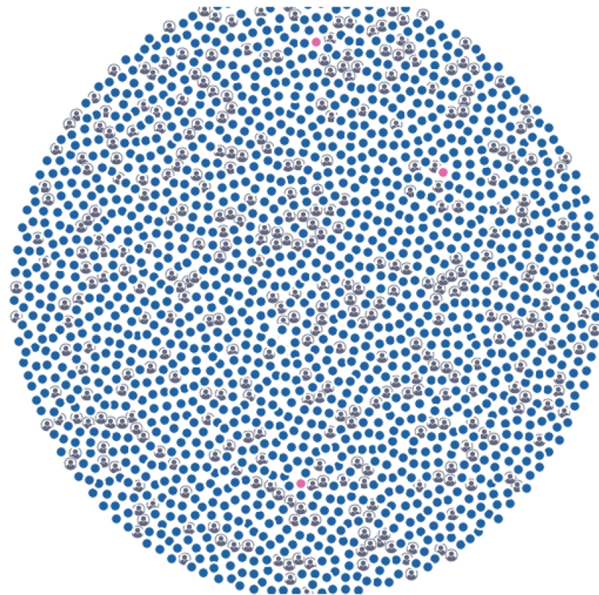
## Graph Network Resources

In addition to the graph of users presented on the **Overview** pane, you can use the **Resource Graph** tab to create a map of the resources inside PAM that are being utilized on the network. The following graph is an example:





Overview Activity Analytics Locations **Resource Graph** Logs


April 29, 2020 – October 29, 2020





Good Normal A Labels  
Suspect Sensitive  
Bad Disconnected

This view includes **Normal** and **Good** resources but also resources that are **Sensitive** and may require further examination. If you select a user in the graph, it opens a **User Quick View** that shows the name of the user, the latest IP address, changes in status, and a list of all the devices used.


 **User Quick View** 


 **super**


 Triggered: May 18, 2022 7:55 PM


 Latest IP Address 10.76.13.123


**USER DEVICES (ALL)**

 e4ad405c1ee6e0a4e880885de4a...

 ae21e73862178c4d3a191afc4837...

 6d9dd9cfb3018209ef7bc85ed915...

 890ea5626a08013db22b69f89836...

 239e1ab7a0c1488e649055c96b9...

You can select an individual user or device and can view its **Risk Level Activity**, including a time line of potentially suspicious activity.

## Review Session Logs

The **Logs** tab on the **Home** menu creates a list of all the events that occurred in the time range that is specified in the upper right drop-down menu.

Overview	Activity	Analytics	Locations	Resource Graph	Logs	April 26, 2022 – May 26, 2022	▼
----------	----------	-----------	-----------	----------------	------	-------------------------------	---

Download as .csv

Timestamp	Type	Object	Description
May 26, 2022 6:38 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:38 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:36 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:36 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:34 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:34 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:32 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:32 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:30 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:30 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:28 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:28 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:26 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:26 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:24 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:24 PM	System	N/A	API enabled - Main Queue is NORMAL
May 26, 2022 6:22 PM	System	N/A	Main Queue processor active - Sync Queue is NORMAL
May 26, 2022 6:22 PM	System	N/A	API enabled - Main Queue is NORMAL

If you select the blue icon in the heading of the **Type** column, you see a list of log types in the table so you can view each type separately. These log types include the following categories:

- **Activity**
- **Analytic Decision**
- **Device User Subject**
- **IP Session**
- **System**
- **Risk Factor Decision**
- **Risk Level Decision.**

The following example type produces a list of Analytic Decisions:

1 Data Filter Transaction Type : AnalyticDecision x

[Download as .csv](#)

Timestamp	Type	Transaction Type	Description
May 26, 2022 3:25 PM	AnalyticDe	Activity Analytic Decision Device User Subject	Analytic - New User Agent/WEEK expired for Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f. Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f accessed a resource with a new User Agent - Apache-HttpClient/4.5.13 (Java/1.8.0_322).
May 23, 2022 8:18 PM	AnalyticDe	IP Session System	Analytic - Concurrent Service Sessions expired for User - super. User - super has more than one active Service Session against Service - CA PAM
May 23, 2022 7:30 PM	AnalyticDe	Risk Factor Decision Risk Level Decision	Analytic - Concurrent Resource Sessions expired for User - super. User - super has more than one active Resource Session initiated from Service - CA PAM
May 23, 2022 7:29 PM	AnalyticDe		Analytic - Concurrent Resource Sessions triggered for User - super. User - super has more than one active Resource Session initiated from Service - CA PAM
May 23, 2022 7:24 PM	AnalyticDecision	super	Analytic - Concurrent Service Sessions triggered for User - super. User - super has more than one active Service Session against Service - CA PAM
May 19, 2022 3:20 PM	AnalyticDecision	3e153242c16a7e73687d08223331...	Analytic - New User Agent/WEEK triggered for Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f. Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f accessed a resource with a new User Agent - Apache-HttpClient/4.5.13 (Java/1.8.0_322).
May 19, 2022 3:20 PM	AnalyticDecision	3e153242c16a7e73687d08223331...	Analytic - New User Agent/DAY triggered for Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f. Device - 3e153242c16a7e73687d082233314dc0cae570b66d49ecacc31dc0f0c1032c8f accessed a resource with a new User Agent - Apache-HttpClient/4.5.13 (Java/1.8.0_322).

If you select the blue “Download as .csv” text block at the top of the left column in the table, the filtered list view can be saved as a \*.csv Excel file for a subsequent reference.

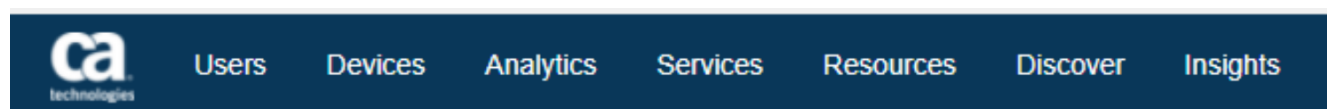
## Investigate Basic Components of the Network

The menu tabs in the bar at the top of the Threat Analytics display provide information about five functional components of the PAM environment:

- **Users:** [Examine Users and Risk Levels](#)
- **Devices:** [Track Analytics for All Devices](#)
- **Analytics:** [View All Analytics and Status Decisions](#)
- **Services:** [Track Activity across All Services](#)
- **Resources:** [Monitor Activity Across All Resources](#)

Two more tabs summarize and interpret this raw data to provide a deeper analysis of potential threats to the network, making them especially useful.

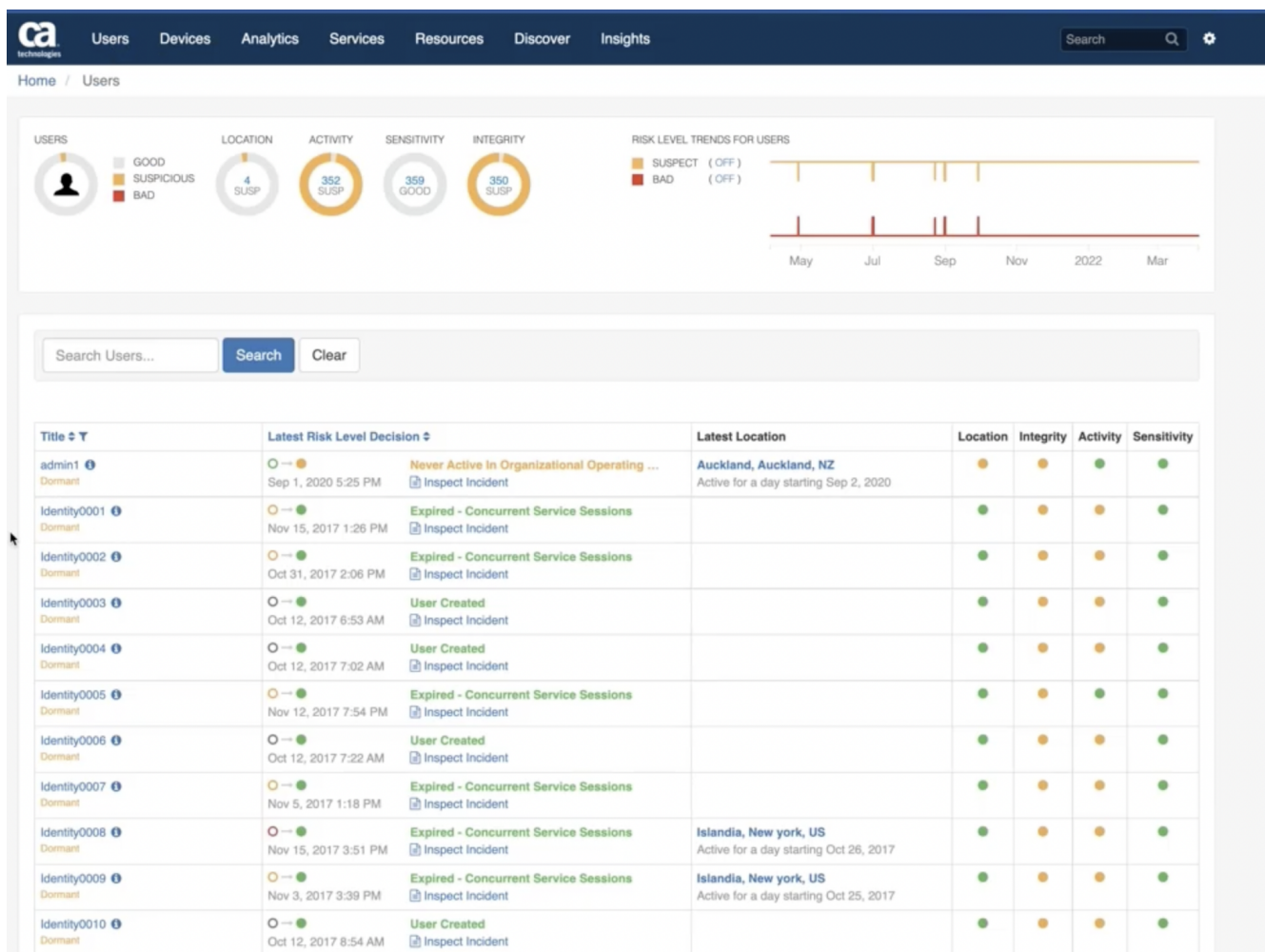
- **Discover:** [Interpret Threats Using the Discover Tab](#)
- **Insights:** [View Data Insights on Network Activity](#)



The first five menu tabs focus on lists of the users, devices, analytics, services, and resources detected as a starting point for analysis. Much of the raw data available on the six **Home** tabs also can be accessed from the seven top-line tabs. Generally the differences between the two sets of tabs are complementary methods of viewing and analyzing potential threats in the PAM environment, rather than separate sets of data.

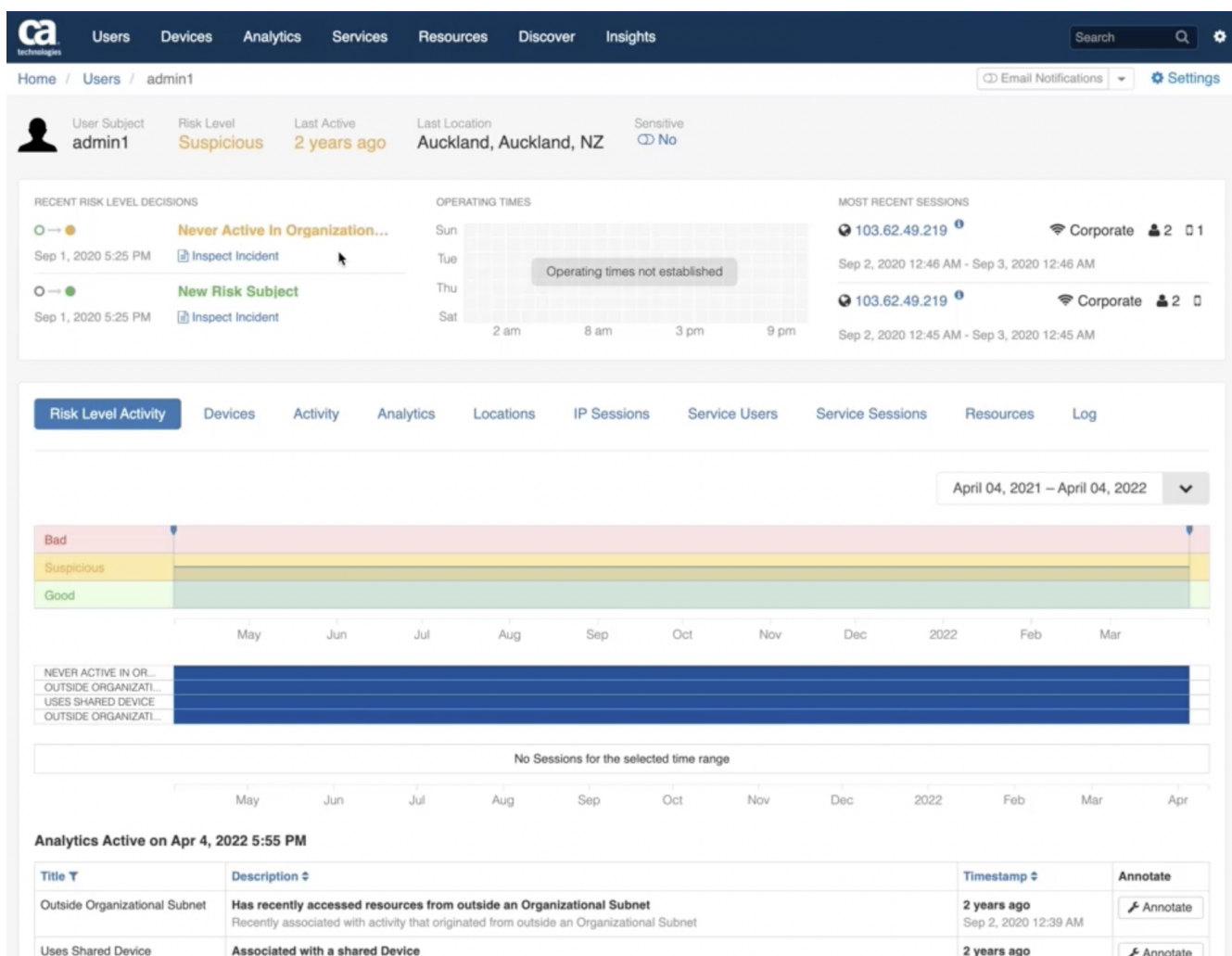
## Examine Users and Risk Levels

The **Users** tab lists all the active users in the PAM environment, their current risk level, their most recent locations, and the current status of the four categories of analytics: **Location**, **Integrity**, **Activity**, and **Sensitivity**. The same status circles seen on the **Overview** tab are reproduced here, and a time line tracks when instances of **Suspect** (yellow-orange) and **Bad** (red) activity have occurred.



Selecting an individual user in the **Title** column, you can view all incidents and analytics on the **Risk Level Activity** pane.

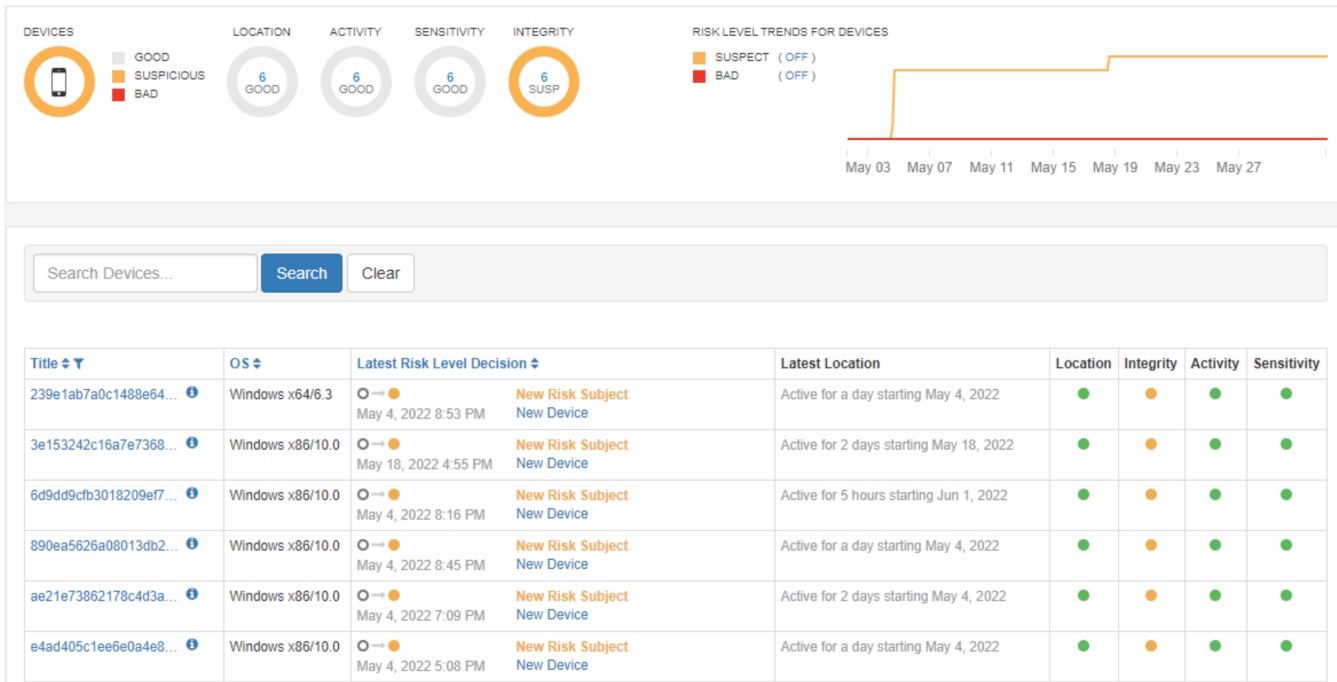




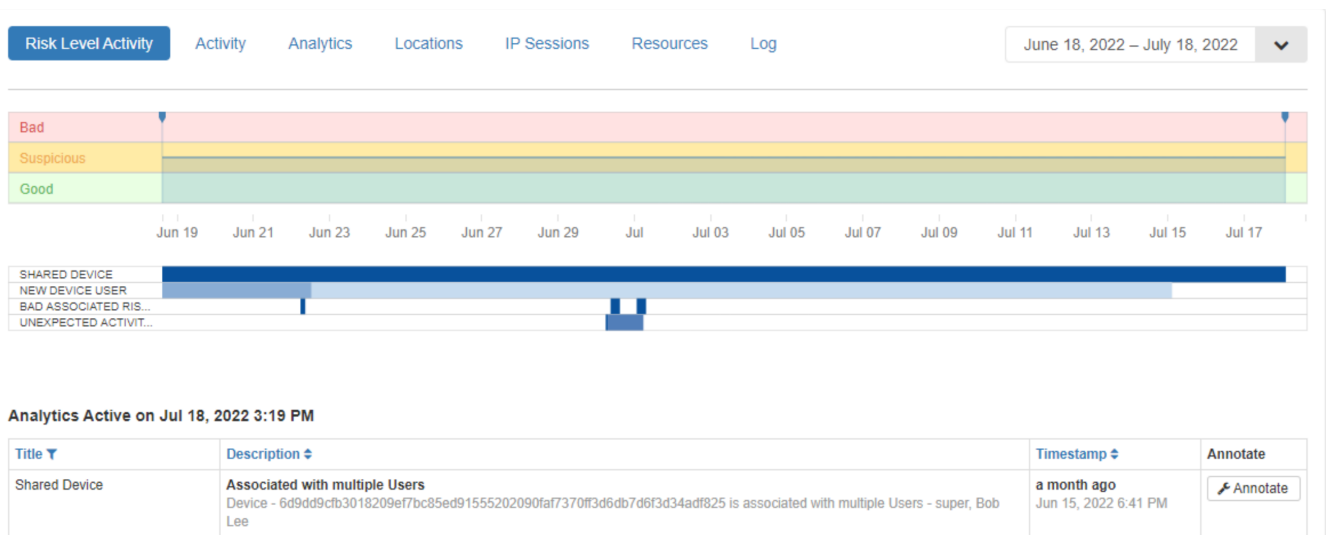
The particular user named “admin1,” shown in the example above has never been active in the organization and has become a new risk suspect. In addition, this user has logged in from an unusual location: Auckland, New Zealand, which has not been previously used. This user has also recently accessed resources that are not part of the organization’s subnet and has also been associated with a shared device. The triggering of these analytics has raised the risk level for this user to **Suspicious**.

## Track Analytics for All Devices

The **Devices** tab lists all the devices that connect to the PAM Appliance through a browser or the PAM client, along with the operating systems they use, latest risk level decisions, locations, and status in each of the four analytic categories. The following example shows six devices being used in the same session. An excessive number of devices could mean that the user is that trying to test multiple addresses to break into the network, which elevates the risk level of the user to **Suspect**.



Selecting a device name displays its risk level in the **Risk Level Activity** window, with a heat map over a time line and all the analytics that caused this risk level escalation. In this case, the device that is used has been associated with multiple users.



For more details about the **Risk Level Activity** window, see [Track Risk Level Activity for all Users and Devices](#).

## View All Analytics and Status Decisions

The **Analytics** tab in the top of the screen lists all 58 analytics that are used by the Threat Analytics Console, reporting the following information:

- The category of the risk factor (**Activity**, **Sensitivity**, **Integrity**, or **Location**)
- The name of the analytic
- Whether the analytic has been triggered, and if so when
- Whether each one was applied and enabled for the user or device
- How many times the analytic has been triggered.

Analytics

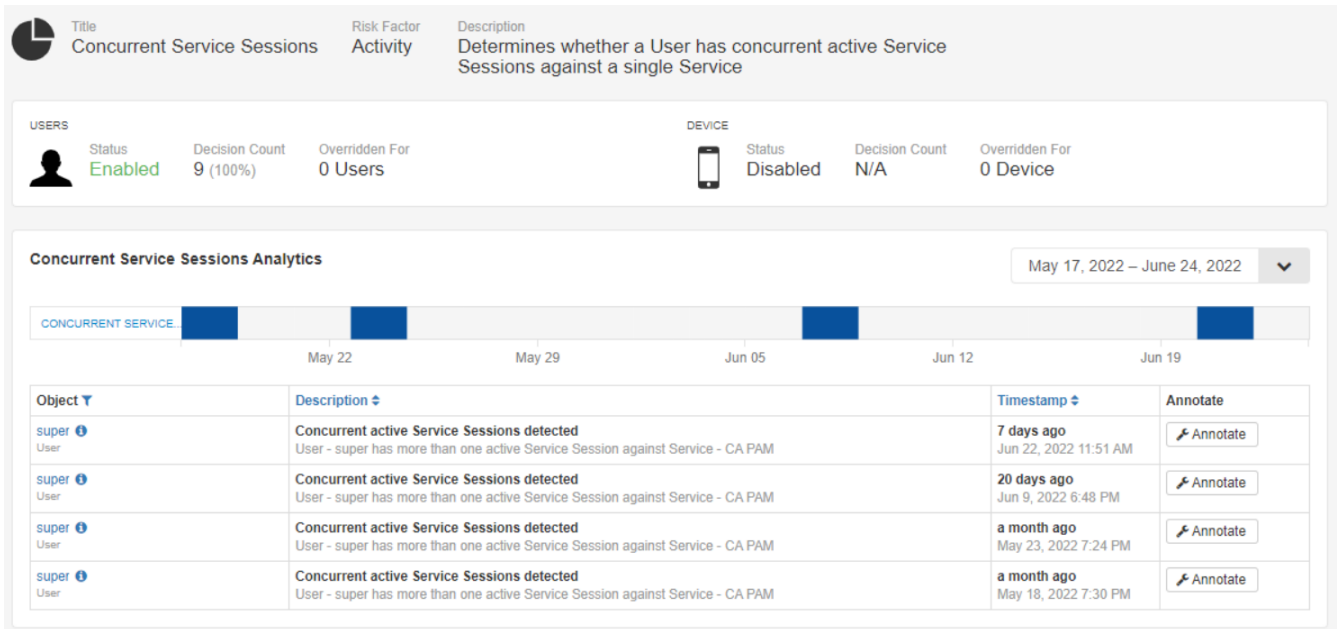
Decisions

May 01, 2022 – June 01, 2022

Risk Factor ▼	Analytic ⚙	Last Triggered	Users	Devices	Triggers ⚙
Activity	<b>Abnormal Resource Session Rate</b> Determines whether a User Subject has an active Service Session with Resource Sessions having been established at an abnormal rate	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Abnormal Resource Session Rate for User Subject</b> Determines whether a User has an active Service Session with Resource Sessions having been established at an abnormal rate for the identity	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Abnormally Long Resource Session</b> Determines whether a User Subject has a resource session that is abnormally long	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Abnormally Long Resource Session For User Subject</b> Determines whether a User Subject has a resource session that is abnormally long for the identity	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Abnormally Long Service Session</b> Determines whether a User Subject has a service session that is abnormally long	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Abnormally Long Service Session for Identity</b> Determines whether a User Subject has a service session that is abnormally long for the identity	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Activity	<b>Access Denials</b> Determines whether a Risk Subject has been denied access to resources on a Service at an unusual rate	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	✓ Applied and Enabled Contributing to devices risk level	No Triggers N/A
Sensitivity	<b>Accessing Sensitive Resource</b> Determines whether a User is actively accessing a Resource that is sensitive	Not Triggered N/A	✓ Applied and Enabled Contributing to users risk level	⊘ Not Applied Not applied to Devices	No Triggers N/A
Integrity	<b>Associated With Deactivated User</b> Determines whether a Device is associated with a User that has been deactivated, disabled, or deleted from an Identity Service	Not Triggered N/A	⊘ Not Applied Not applied to Users	✓ Applied and Enabled Contributing to devices risk level	No Triggers N/A
Integrity	<b>Bad Associated Risk Subject</b>	14 days ago May 18, 2022 7:30 PM	✓ Applied and Enabled Contributing to users risk level	✓ Applied and Enabled Contributing to devices risk level	6 0% Users, 100% Devices

In contrast, the **Analytics** tab on the **Overview** menu only shows the analytics that were triggered during a specific session.

You can select each analytic to see more information. This example displays four instances of the “Concurrent Service Sessions” analytic in the past month, revealing that a user was detected using more than one active service session simultaneously.



The **Annotate** buttons in the right-most column that can be used to report any relevant information that is uncovered after the incident, similar to what was previously described in the **Risk Level Activity** table for the analytic.

The **Analytics** menu tab also has a **Decisions** tab. This tab reports more details of all the analytics that are triggered within a specified time period. The user and device names appear in the **Object** column, as is the date when a triggered analytic occurred. You can select the analytic decisions that are listed on the left of the heat map timeline to discover all the details of that particular analytic decision.

[Users](#)
[Devices](#)
[Analytics](#)
[Services](#)
[Resources](#)
[Discover](#)
[Insights](#)

[Home](#) / [Analytics](#)

[Analytics](#)
[Decisions](#)

April 29, 2020 – October 29, 2020

**Analytic Decisions** ( Apr 29, 2020 5:56 PM - Oct 29, 2020 5:56 PM )

CONCURRENT SERVICE...

NEW RISK SUBJECT

NONSTANDARD USER D...

NEW USER OPERATING...

NEW USER DEVICE FA...

NEW USER DEVICE

USES SHARED DEVICE

NEW DEVICE USER

NEW USER AGENT

UNEXPECTED ACTIVIT...

SHARED DEVICE

ACCESSING SENSITIV...

EXCESS RESOURCE SE...

OUTSIDE ORGANIZATI...

USER DEVICE COUNT ...

USER DEVICE COUNT ...

DORMANT

ABNORMALLY LONG RE...

CONCURRENT RESOURC...

WITHIN ORGANIZATIO...

Title ▼	Object ▼	Description ↕	Timestamp ↕	Annotate
Accessing Sensitive Resource	super	<b>Accessing a Resource that has been marked as sensitive</b> User - super is actively accessing one or more resources that has been marked as sensitive	<b>a year ago</b> Oct 29, 2020 4:53 PM	Annotate
Concurrent Service Sessions	super	<b>Concurrent active Service Sessions detected</b> User - super has more than one active Service Session against Service -	<b>a year ago</b> Oct 29, 2020 4:53 PM	Annotate
Excess Resource Sessions	super	<b>Resource session count abnormally high</b> User has created Resource Sessions in a single Service Session, significantly more than the expected number for the population ()	<b>a year ago</b> Oct 29, 2020 4:53 PM	Annotate
New User Agent	74180c1d23446c54489167f4774...	<b>New User Agent Detected</b> Device - 74180c1d23446c54489167f4774878426aec4a7440725a229cb8b751e54bd7ea accessed a resource with a new User Agent - Apache-HttpClient/4.3.4 (java 1.5).	<b>a year ago</b> Oct 29, 2020 2:54 PM	Annotate
New Risk Subject	74180c1d23446c54489167f4774...	<b>New Device</b> This Device was added at 2020-10-29 14:50:47 UTC.	<b>a year ago</b> Oct 29, 2020 2:50 PM	Annotate
Unexpected Activity Time	super	<b>Generated activity outside of the normal operating time</b> Activity count significantly exceeded expected maximum for this time of day	<b>a year ago</b> Oct 29, 2020 1:50 PM	Annotate
New User Device	super	<b>New User Device detected</b> User - super was detected using Device - 423a48a4c15d072fdb5e596ba454d487fab1a3aa1fed0c26aa9631263255c34, which the User has not previously used.	<b>a year ago</b> Oct 29, 2020 1:50 PM	Annotate
Concurrent Service Sessions	andje01@forwardinc.ca	<b>Concurrent active Service Sessions detected</b> User - andje01@forwardinc.ca has more than one active Service Session against Service - CA PAM	<b>a year ago</b> Oct 28, 2020 9:11 PM	Annotate
Concurrent Service Sessions	andje01@forwardinc.ca	<b>Concurrent active Service Sessions detected</b> User - andje01@forwardinc.ca has more than one active Service Session against Service - CA PAM	<b>a year ago</b> Oct 28, 2020 9:10 PM	Annotate
Concurrent Service Sessions	andje01@forwardinc.ca	<b>Concurrent active Service Sessions detected</b> User - andje01@forwardinc.ca has more than one active Service Session against	<b>a year ago</b> Oct 28, 2020 9:09 PM	Annotate

Similarly, if you select a device in the **Object** column of the main **Analytic** table, you can see an assessment of **Risk Level Activity** for devices that have questionable status.

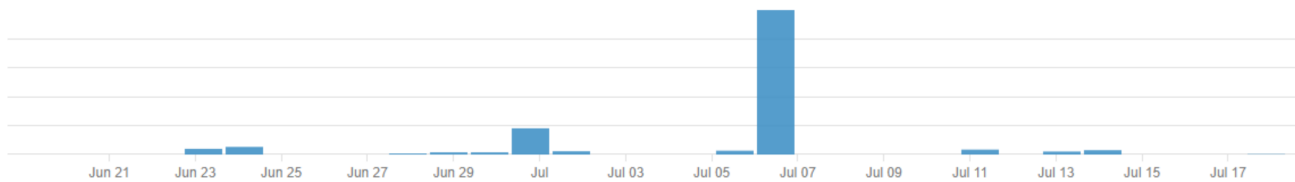
## Track Activity across All Services

The **Services** tab records the activity of all services that were used over a specified time period, showing your connections to the Privileged Access Manager. The only service in use for this example is the CA PAM client application. This tab is most often used to set up an environment and is not typically accessed daily.

[Home](#) / [Services](#)

ACTIVITY ACROSS ALL SERVICES

June 18, 2022 – July 18, 2022



Search Services...

Search

Clear

Service	Health	Identifier	Adapter	Mitigations	Data Caching Enabled	Last Cache	Next Cache
CA PAM	Healthy	74a0acb7-66d7-4178-942d-d355b8f04243	Capam Adapter	Enabled	✓	Jul 18, 2022 4:30 PM	Jul 19, 2022 4:30 AM

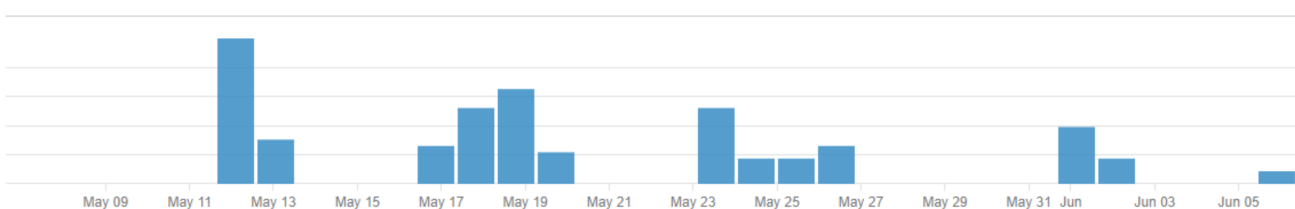
Selecting the name of this service (in this case, CA Privileged Access Manager) displays the first of four services menu tabs, **Activity**. This tab displays a list of service activity, with the following columns:

- Timestamps (UTC)
- Users
- Devices
- Actions and resources
- IP addresses
- The clients involved

Title: CA PAM  
 Identifier: 74a0acb7-66d7-4178-942d-d355b8f04243  
 Adapter Name: Capam Adapter  
 Health State: Healthy

[Activity](#)
[Service Users](#)
[Resources](#)
[Service Sessions](#)

May 06, 2022 – June 06, 2022



Timestamp (UTC) ↕	User ↕	Device ↕	Action - Resource	IP/Location	Client
06/06/2022 18:53:02 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
06/06/2022 18:52:26 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
06/02/2022 20:47:49 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	LOGOUT - CA PAM ⓘ	10.76.13.123 ⓘ	Chrome 90.0.4430.93
06/02/2022 20:47:25 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO_LOGOUT - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
06/02/2022 18:33:32 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
06/02/2022 18:33:11 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
06/01/2022 20:52:03 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	LOGOUT - CA PAM ⓘ	10.76.13.123 ⓘ	Chrome 90.0.4430.93
06/01/2022 20:51:49 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO_LOGOUT - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java

The **Service Users** tab lists all the users for that particular service.

Activity	Service Users	Resources	Service Sessions	Auth Tokens	Configuration
----------	---------------	-----------	------------------	-------------	---------------

Title	Identifier	Service	User Subject Title	Active
Bob Lee	7001	CA PAM	Bob Lee ⓘ	✓
CATapApiUser	2001	CA PAM	CATapApiUser ⓘ	✓
DSApiUser	4001	CA PAM	DSApiUser ⓘ	✓
LDAPApiUser	5001	CA PAM	LDAPApiUser ⓘ	✓
MCApiUser	1001	CA PAM	MCApiUser ⓘ	✓
Sam Grant	6001	CA PAM	Sam Grant ⓘ	✓
super	1	CA PAM	super ⓘ	✓

The **Resources** tab lists all the PAM resources that are used by the service, and the identifiers used.

Activity	Service Users	Resources	Service Sessions	Auth Tokens	Configuration
----------	---------------	-----------	------------------	-------------	---------------

Service	Title	Identifier	Sensitive
CA PAM	apikey.xceedium.com ⓘ	21001	
CA PAM	CA PAM ⓘ	74a0acb7-66d7-4178-942d-d355b8f04243	
CA PAM	ca.portal.azure.com ⓘ	18001	
CA PAM	nim.pam.ca.com ⓘ	17001	
CA PAM	server.control.policies.pam ⓘ	23001	
CA PAM	tap.ca.com ⓘ	22001	
CA PAM	TAPDummy ⓘ	24001	
CA PAM	xceedium.aws.amazon.com ⓘ	19001	

The **Service Sessions** tab provides details about the service sessions. This tab displays a list of all services activity, with the following columns for each entry:

- The user of the session
- Details about the session
- The start and end times
- The duration of each session
- The count of resource sessions

Activity	Service Users	Resources	Service Sessions	Auth Tokens	Configuration
----------	---------------	-----------	------------------	-------------	---------------

June 20, 2022 – July 20, 2022 ▼

Service	User	Service Session	Session Start	Session End	Session Duration	Resource Sessions Count
CA PAM	super ⓘ	Session Details ⓘ	Jul 20, 2022 6:14 PM	Active	496 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 20, 2022 3:04 PM	Jul 20, 2022 4:06 PM	3689 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 19, 2022 7:33 PM	Jul 19, 2022 8:32 PM	3557 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 18, 2022 7:18 PM	Jul 18, 2022 8:40 PM	4878 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 14, 2022 6:05 PM	Jul 14, 2022 8:33 PM	8901 Sec	4
CA PAM	super ⓘ	Session Details ⓘ	Jul 14, 2022 3:42 PM	Jul 14, 2022 4:28 PM	2786 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 13, 2022 6:11 PM	Jul 13, 2022 8:26 PM	8102 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 13, 2022 2:17 PM	Jul 13, 2022 3:50 PM	5572 Sec	2
CA PAM	super ⓘ	Session Details ⓘ	Jul 11, 2022 7:08 PM	Jul 11, 2022 8:42 PM	5628 Sec	3
CA PAM	super ⓘ	Session Details ⓘ	Jul 11, 2022 5:09 PM	Jul 11, 2022 7:08 PM	7133 Sec	1
CA PAM	super ⓘ	Session Details ⓘ	Jul 11, 2022 2:52 PM	Jul 11, 2022 4:37 PM	6316 Sec	2
CA PAM	super ⓘ	Session Details ⓘ	Jul 5, 2022 6:17 PM	Jul 5, 2022 8:46 PM	8940 Sec	4

You can select any of the blue “Session Details” links (in the third column) to see the following listed on the **Activities** submenu tab:

- Each timestamp of each activity
- The user
- Devices
- Actions that are taken and resources that are used
- The IP or location
- The client used

Activities Resource Sessions					
Timestamp (UTC) ↕	User ↕	Device ↕	Action - Resource	IP/Location	Client
05/24/2022 19:51:05 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	LOGOUT - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
05/24/2022 19:50:14 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO_LOGOUT - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
05/24/2022 17:23:58 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
05/24/2022 17:23:21 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13

Select the **Resource Sessions** submenu tab to display a table with following data:

- The service used
- The user name
- The resource name
- Resource session details
- The start and end times of each session
- The session duration in seconds

Activities Resource Sessions						
Service	User	Resource	Resource Session	Session Start	Session End	Session Duration
CA PAM	super ⓘ	tap.ca.com ⓘ	Session Details ⓘ	May 26, 2022 6:39 PM	May 26, 2022 8:09 PM	5433 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	Session Details ⓘ	May 26, 2022 6:00 PM	May 26, 2022 6:39 PM	2310 Sec

The **Auth Tokens** tab shows the authenticated token for the PAM instance and lists the name (the IP address), the creator, a timestamp, an active/inactive checkbox, and a “Deactivate” button.

Activity Service Users Resources Service Sessions Auth Tokens Configuration				
+ New Auth Token				
Name	Created by	Timestamp	Active	Actions
10.17.40.159 Token for PAM instance 10.17.40.159	admin admin@localhost.local	May 4, 2022 4:31 PM	✓	Deactivate

The **Configuration** tab shows the host IP address of the CA PAM service, the user name, and the password.



Activity Service Users Resources Service Sessions Auth Tokens **Configuration**

## CA PAM Adapter Configuration

Host


Username

Password

Reset Test Save Configuration

## Monitor Activity Across All Resources

The **Resources** tab in the top menu lists all the resources that are used by the PAM network.

 Users Devices Analytics Services Resources Discover Insights			
Home / Resources			
<input type="text" value="Search Resources..."/> Search Clear			
Service	Title	Identifier	Sensitive
CA PAM	apikey.xceedium.com ⓘ	21001	
CA PAM	CA PAM ⓘ	74a0acb7-66d7-4178-942d-d355b8f04243	
CA PAM	ca.portal.azure.com ⓘ	18001	
CA PAM	nim.pam.ca.com ⓘ	17001	
CA PAM	server.control.policies.pam ⓘ	23001	
CA PAM	tap.ca.com ⓘ	22001	
CA PAM	xceedium.aws.amazon.com ⓘ	19001	
CA PAM	xceedium.nsx.vmware.com ⓘ	20001	

Selecting a particular resource can help you uncover all the risky activities that resource participated in. There are four tabs on this window, the first of which (**Users**) lists all the users detected.

Titletap.ca.com

Identifier22001

Sensitive ResourceNo

Users

Devices


Activities

Resource Sessions

Title	Latest Risk Level Decision	Latest Location	Location	Integrity	Activity	Sensitivity
super	<div><div><div></div><div></div></div><div>Expired - Concurrent Service Sessions</div><div>May 18, 2022 7:55 PM</div><div>Inspect Incident</div></div>		<div></div>	<div></div>	<div></div>	<div></div>


The **Devices** tab shows all the devices that triggered analytics and includes data on the operating system that is used, the latest risk level decision, the latest location, and a risk assessment for all four categories of analytics (**Location**, **Integrity**, **Activity**, and **Sensitivity**).

Users **Devices** Activities Resource Sessions

Title ▾	OS ▾	Latest Risk Level Decision ▾	Latest Location	Location	Integrity	Activity
239e1ab7a0c1488e64... <small>Dormant</small>	Windows x64/6.3	 →  Jul 1, 2022 5:31 PM <b>Expired - Bad Associated Risk Sub...</b> Associated with a bad User	Active for a day starting May 4, 2022			
26868d1635154b104a... <small>Dormant</small>	Windows x86/10.0	 →  Jun 23, 2022 8:41 PM <b>New Risk Subject</b> <b>New Device</b>	Active for a day starting Jun 23, 2022			
3e153242c16a7e7368... <small>Dormant</small>	Windows x86/10.0	 →  Jul 1, 2022 5:31 PM <b>Expired - Bad Associated Risk Sub...</b> Associated with a bad User	Active for 2 days starting May 18, 2022			
6d9dd9cfb3018209ef7... <small>Dormant</small>	Windows x86/10.0	 →  Jun 15, 2022 6:41 PM <b>New Device User</b> <b>New Device User detected</b>	Active for 2 days starting Jul 18, 2022			
890ea5626a08013db2... <small>Dormant</small>	Windows x86/10.0	 →  Jul 1, 2022 5:31 PM <b>Expired - Bad Associated Risk Sub...</b> Associated with a bad User	Active for a day starting May 4, 2022			

The **Activities** tab of the **Resource** menu lists all the activities that occurred, with the following columns:

- The UTC timestamp
- The user
- The device
- The particular activity that is detected and resource that is used
- The IP/location
- The client

Title	Identifier	Sensitive Resource
CA PAM	74a0acb7-66d7-4178-942d-d355b8f04243	 No

Users	Devices	<b>Activities</b>	Resource Sessions
-------	---------	-------------------	-------------------

Timestamp (UTC) ▾	User ▾	Device ▾	Action - Resource	IP/Location	Client
06/02/2022 18:33:11 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN - CA PAM	10.76.13.123	Other Library 4.5.13
06/01/2022 20:52:03 <small>Service Session</small>	super	6d9dd9cfb3018209ef7bc85ed9155... <small>Dormant</small>	LOGOUT - CA PAM	10.76.13.123	Chrome 90.0.4430.93
06/01/2022 19:06:22 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN - CA PAM	10.76.13.123	Other Library 4.5.13
06/01/2022 19:06:13 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN_FAILURE - CA PAM	10.76.13.123	Other Library 4.5.13
06/01/2022 15:57:21 <small>Service Session</small>	super	6d9dd9cfb3018209ef7bc85ed9155... <small>Dormant</small>	LOGOUT - CA PAM	10.76.13.123	Chrome 90.0.4430.93
06/01/2022 15:08:22 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN - CA PAM	10.76.13.123	Other Library 4.5.13
05/26/2022 20:09:52 <small>Service Session</small>	super	6d9dd9cfb3018209ef7bc85ed9155... <small>Dormant</small>	LOGOUT - CA PAM	10.76.13.123	Chrome 90.0.4430.93
05/26/2022 17:59:23 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN - CA PAM	10.76.13.123	Other Library 4.5.13
05/25/2022 20:05:10 <small>Service Session</small>	super	6d9dd9cfb3018209ef7bc85ed9155... <small>Dormant</small>	LOGOUT - CA PAM	10.76.13.123	Other Library 4.5.13
05/25/2022 18:28:13 <small>Service Session</small>	super	Other (Other) running Other 1.8.0_3... <small>Dormant</small>	LOGIN - CA PAM	10.76.13.123	Other Library 4.5.13
05/24/2022 19:51:05 <small>Service Session</small>	super	6d9dd9cfb3018209ef7bc85ed9155... <small>Dormant</small>	LOGOUT - CA PAM	10.76.13.123	Other Library 4.5.13

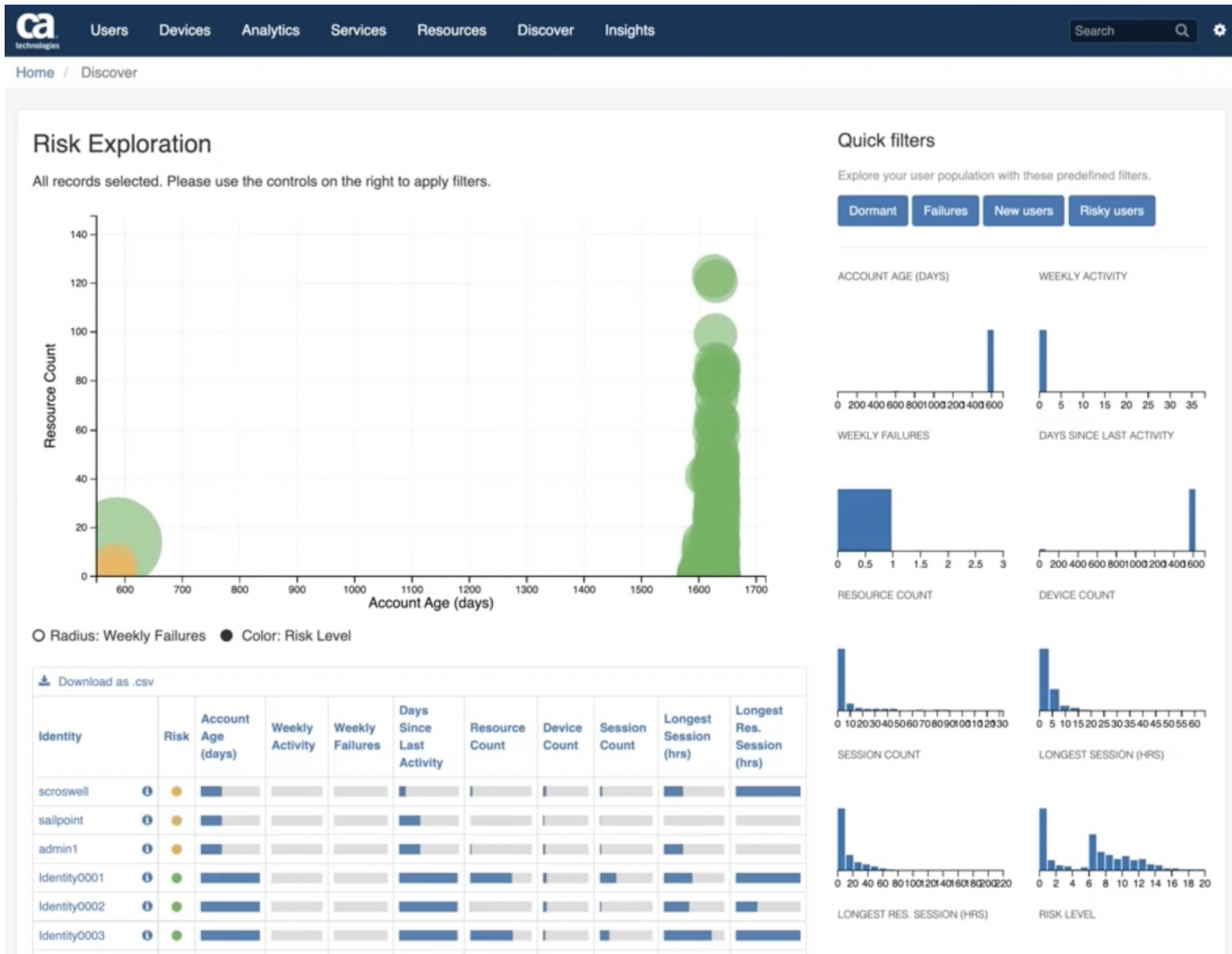
The **Resource Sessions** tab lists every session for a particular user or service, including session details.

<a href="#">Users</a> <a href="#">Devices</a> <a href="#">Activities</a> <a href="#">Resource Sessions</a>							
Service	User	Resource	Resource Session	Service Session	Session Start	Session End	Session Duration
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	Jun 6, 2022 6:53 PM	Active	6521 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	Jun 2, 2022 6:33 PM	Jun 2, 2022 8:47 PM	8033 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	Jun 1, 2022 7:06 PM	Jun 1, 2022 8:51 PM	6310 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	Jun 1, 2022 3:08 PM	Jun 1, 2022 3:57 PM	2909 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	May 26, 2022 6:39 PM	May 26, 2022 8:09 PM	5433 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	May 26, 2022 6:00 PM	May 26, 2022 6:39 PM	2310 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	May 25, 2022 6:28 PM	May 25, 2022 8:03 PM	5688 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	May 24, 2022 5:23 PM	May 24, 2022 7:50 PM	8776 Sec
CA PAM	super ⓘ	tap.ca.com ⓘ	<a href="#">Session Details ⓘ</a>	<a href="#">Session Details ⓘ</a>	May 23, 2022 7:29 PM	May 23, 2022 7:30 PM	26 Sec

## Interpret Threats Using the Discover Tab

The **Discover** tab in the top row of menus provides an overview of network activity. This tab displays the following features:

- A visual map of traffic over a timeline with **Suspect** and **Bad** activity color-coded (top left)
- A sortable and exportable filtered list of identities (bottom left)
- A set of ten **Quick filters** that display the age of an account, its weekly activity, weekly failures, and days since the last activity. They also include graphs of the resource count, the device count, and the session count, as well as the longest session (in hours), the longest resource session, and the overall risk level.



When you open the **Discover** page for the first time, you see data based on all the users on the network. The main graph on this page is entitled **Risk Exploration** and it shows the risk activity for all selected records. The four tabs on the upper right side toggle the **Quick Filters** through four types of users:

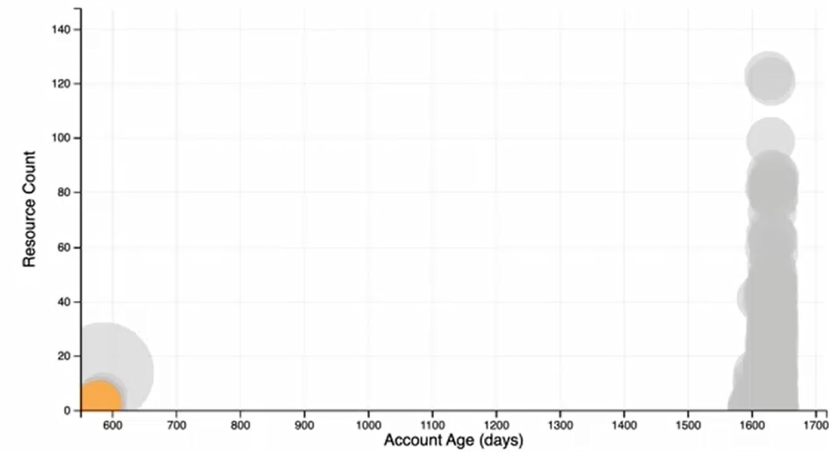
- **Dormant** (no recent activity)
- **Failures** (users with the most weekly failures)
- **New Users**
- **Risky Users**

Each of the 10 graphs and the map change for each user group selected. You can save and then print the list of identities table for reports by selecting the "Download as .csv" link in the top row.

The following example graph displays a resource count, showing how many targets the users are connecting to versus the age of their account. The yellow-orange area at the left of the time line reveals some suspicious activity. This user has only had the account for a short period but has connected with a high number of resources. You can select that area to bring up the particular user and get more insight into why the analytics were triggered.

## Risk Exploration

1 selected out of 359 records | [Reset All](#)



○ Radius: Weekly Failures ● Color: Risk Level

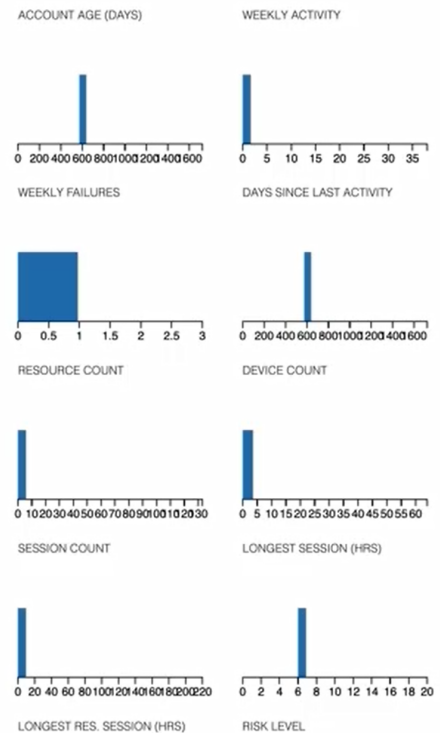
[Download as .csv](#)

Identity	Risk	Account Age (days)	Weekly Activity	Weekly Failures	Days Since Last Activity	Resource Count	Device Count	Session Count	Longest Session (hrs)	Longest Res. Session (hrs)
admin1										

### Quick filters

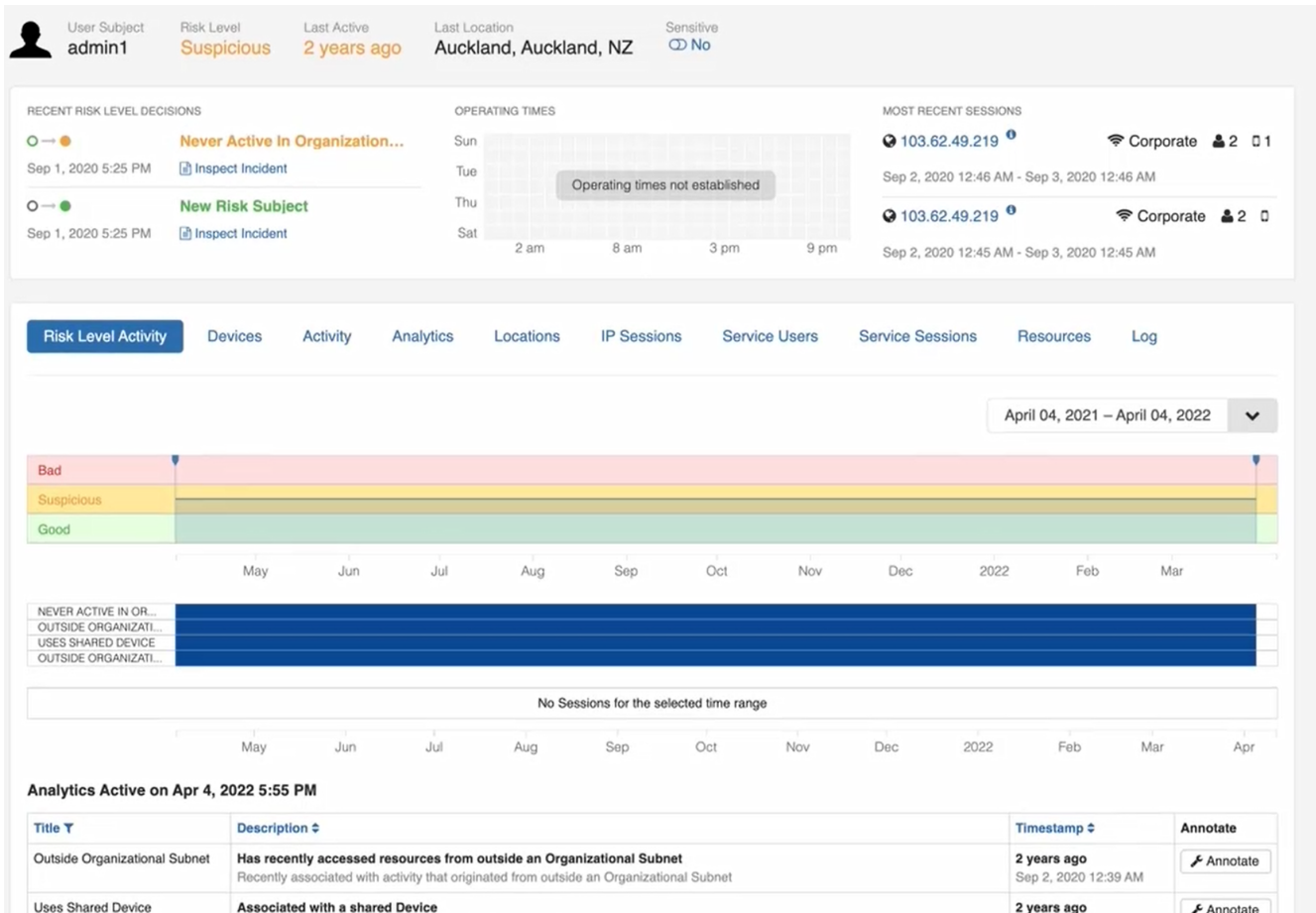
Explore your user population with these predefined filters.

[Dormant](#) [Failures](#) [New users](#) [Risky users](#)



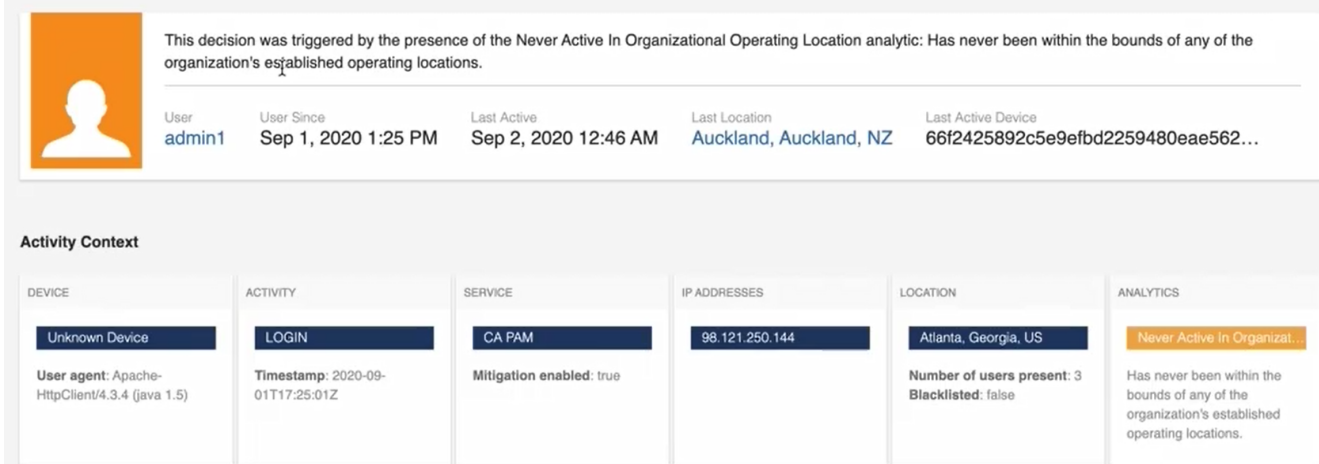
The **Quick Filters** on the right side also show more-specific graphs of the suspect user activity. This analysis might correspond to a server admin logging into many different servers to perform installations or patches, and may not be a threat. But it could be evidence of a breached account that is being used to steal data. Selecting one of the four **Quick Filters** tabs updates all the tables on the page, revealing statistics for dormant users, users with login failures, new users, and risky users. To return to the opening page of the **Discover** tab, select **Reset All** under the **Risk Exploration** title.

To view the **Risk Level Activity** page for the suspect user in this example, select the yellow-orange circle in the lower left portion of the **Risk Exploration** graph.



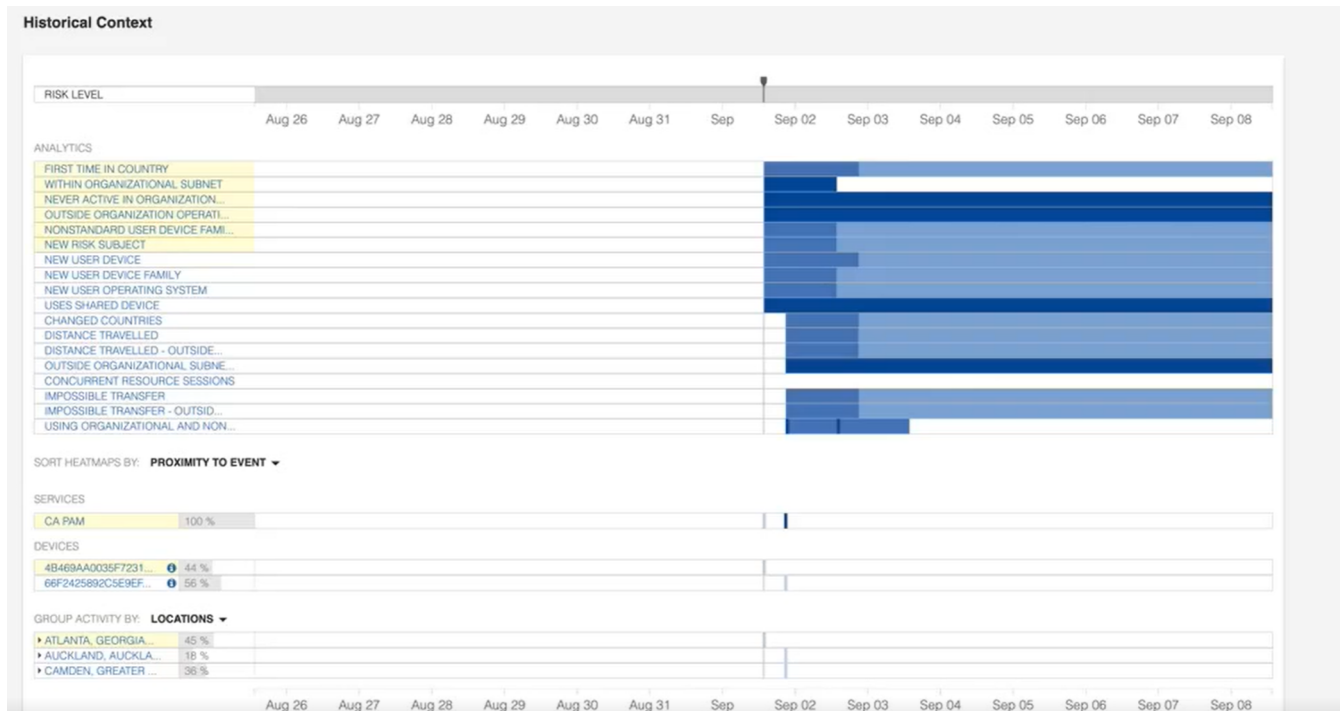
In this example, you can see in the summary pane that the "Never Active in Organization" analytic was triggered for the entire time line. Select the blue **Inspect Incident** link under the "Never Active in Organizational Operating Location" analytic at the top of the screen to display a report on that particular analytic decision:

### User admin1 changed from Good to Suspicious on Sep 1, 2020 5:25 PM



The **Risk Level Activity** page also displays a **Historical Context** table that provides information on past activity by the suspected "admin1" user. This table can be used in different ways:

- To help verify that the user has traveled to remote locations
- To determine when the analytics kicked in
- To obtain the different IP addresses used
- What services, devices, and locations were involve



If you need to share these insights with other team members or managers, select the blue “Export to PDF” link in the header of the **Inspect Incident** report (on the main **Risk Level Activity** page). The Threat Analytics Console allows you to collect and correlate all the data without having to contact other sources.

## View Data Insights on Network Activity

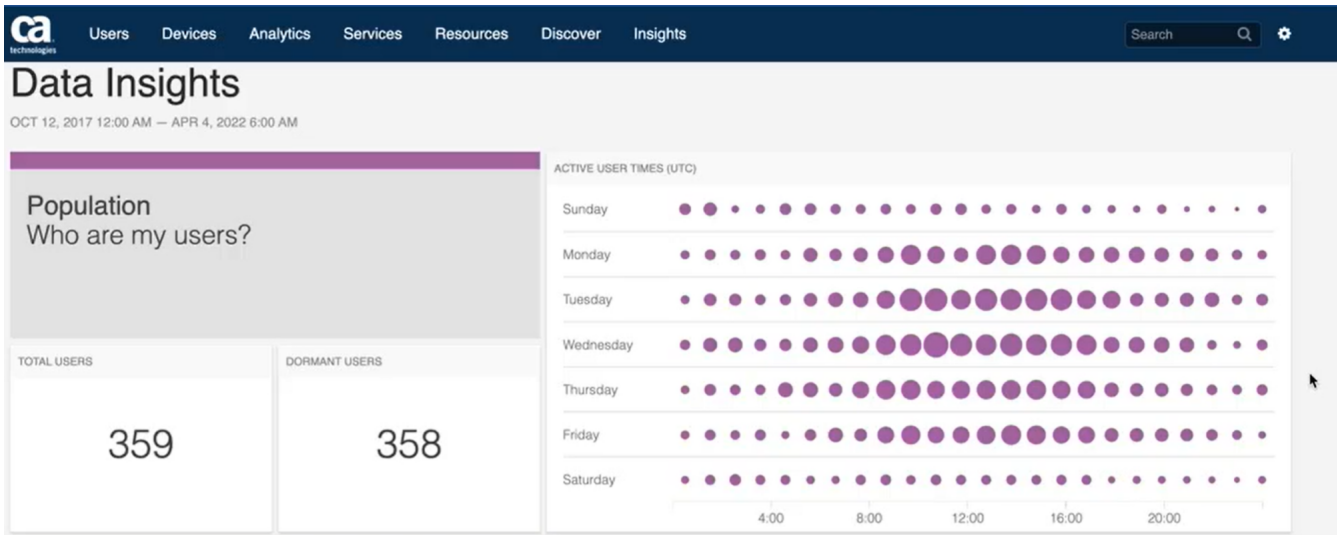
The **Data Insights** menu tab assembles key summary data for all PAM operations by deploying an array of statistics, maps, and graphs. This tab is divided into the following five sections:

- [Population: Who Are My Users?](#)
- [Location: Where Are My Users?](#)
- [Activity: How Are the Users Operating?](#)
- [Risk: How Risky Are my Users?](#)
- [Devices: Which Devices Are Being Used?](#)

### Population: Who Are My Users?

The **Population** section totals up all current and dormant users and provides a graph showing active user time, the busiest days of the week, and the busiest times of day. The larger the circles, the more traffic has been detected. The **Population** section also shows how many dormant users there are on the network. In the following example, there is a large percentage of dormant users, and you should examine them for possible decommission.



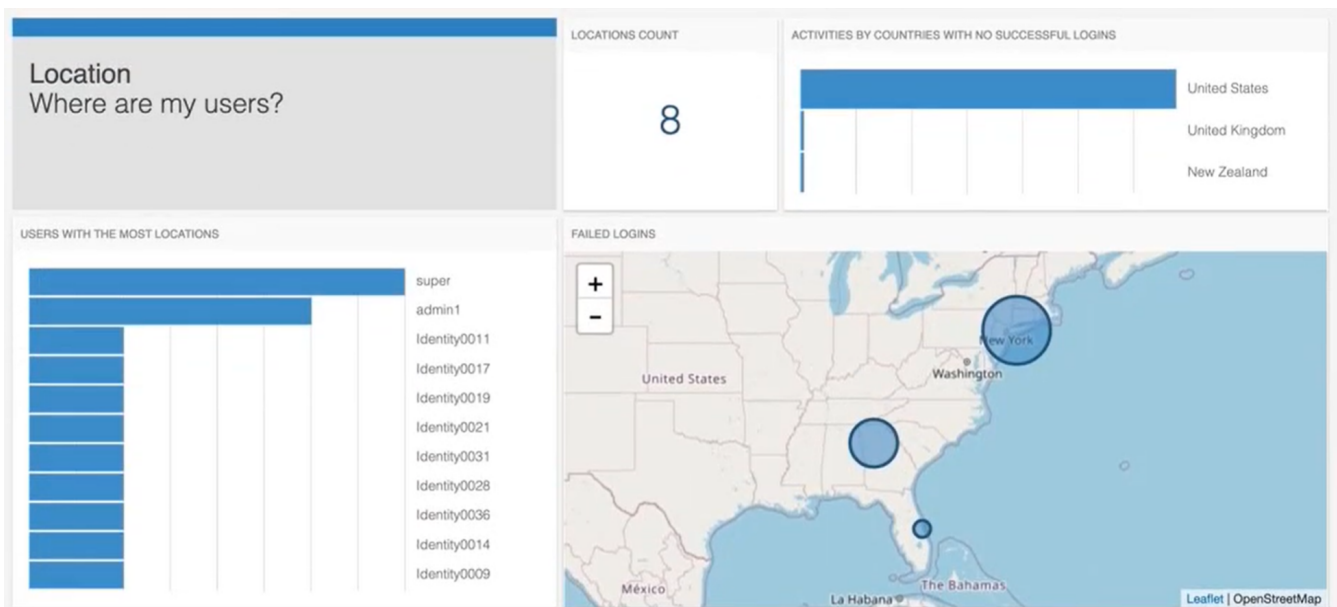


### Location: Where Are My Users?

The **Location** section helps answer the question, “Where are my users?” The section provides these statistics:

- The total number of locations in the network
- All activities from countries with no successful logins
- A list of users with the most locations
- A map of all these detected locations

A user with an unusually high number of locations could be a compromised account that has been sold many times on the dark web. But this high number could also be someone who frequently travels to different company sites.



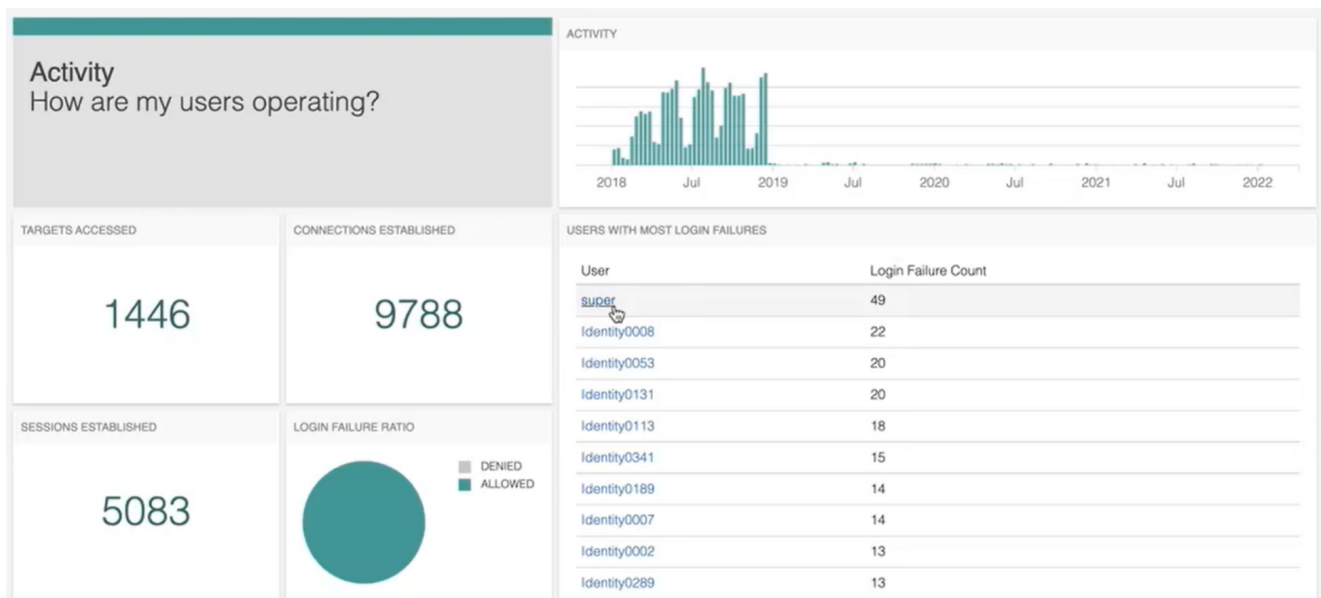
### Activity: How Are the Users Operating?

The **Activity** section of the **Insights** tab analyzes how users are operating. In the following example graphic, we see a network with 1446 different accessed devices, but with 9,788 device connections established. These numbers result in an



average of 6.77 devices per user, which is high. Some of these non-accessed devices could possibly become a source of potential attacks and you may want to consider decommissioning them.

The **Activity** section also lists the PAM network users with the most login failures. Typically these users should be rare because PAM manages logins. The following example shows a user with 49 login failures, and these failures could correlate to someone trying to brute-force an account. You can look for other alerts of this kind of activity and what IP addresses the account is trying log into.

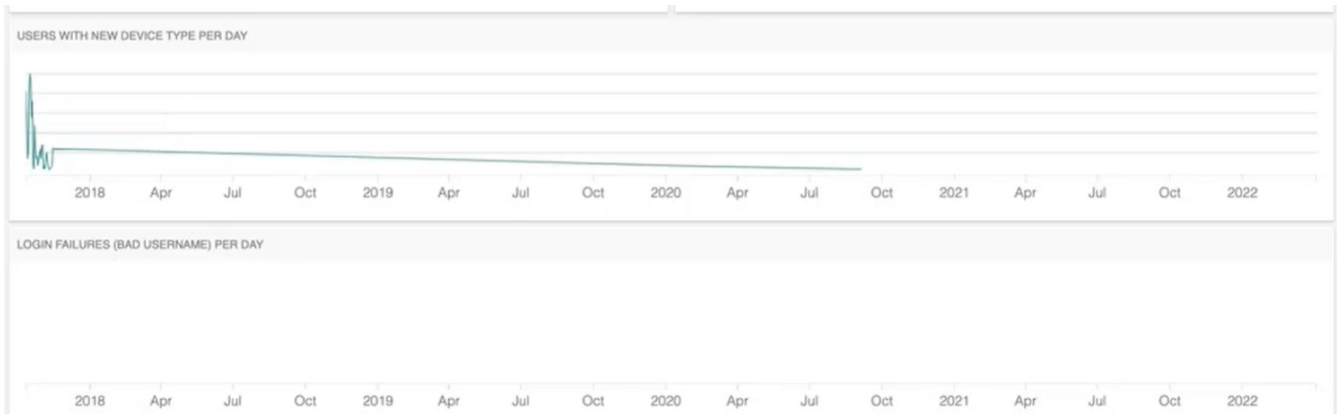


The **Activity** section also lists users with the most resources. The following example shows a user who is associated with 123 resources. This user may be a server admin using PAM to log into servers to patch software or a help desk that is connected to the endpoints of many users. But it could also be a compromised account being used to undertake a lateral move to attack other devices on the network.

USERS WITH MOST RESOURCES		USERS WITH LONGEST SESSIONS	
User	Resources	User	Session Length
Identity0175	123	Identity0036	19:10:47
Identity0066	121	Identity0088	17:52:20
Identity0111	99	Identity0183	16:32:00
Identity0068	87	Identity0086	16:21:04
Identity0003	86	Identity0042	15:38:20
Identity0001	84	Identity0026	15:36:43
Identity0041	83	Identity0003	15:17:02
Identity0167	82	Identity0096	14:53:08
Identity0054	82	Identity0076	14:51:53
Identity0067	81	Identity0010	14:28:31

The **Activity** section also tracks the users with the longest sessions. Typically, PAM console sessions are set to time out and should not be taking 14 through 19 hours like the 10 users who are shown in this example. This activity could warrant further examination about what systems the users have logged into and whether someone has bypassed the time-out restrictions.

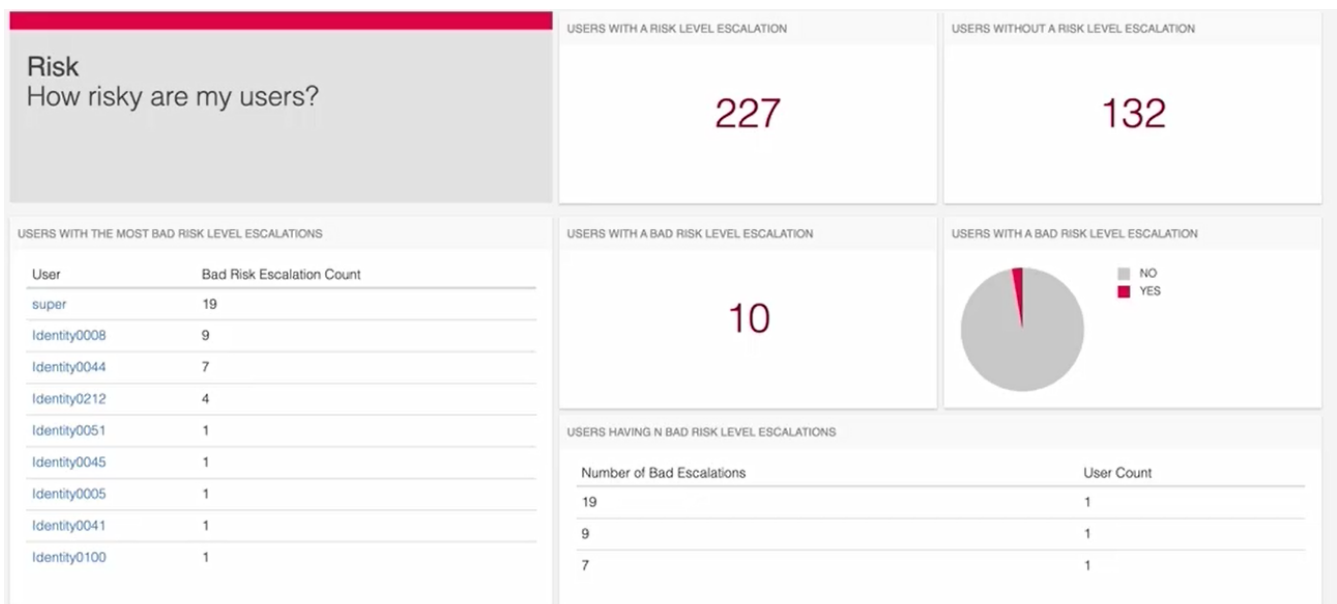
Two graphs complete the **Activity** section. One is **Users with New Device Type per Day**, valuable for networks that allow users to use their own personal devices (BYOD). Typically new device types spike after holiday periods, when users get a new phone or tablet device. Generally, new device activity should trend down after such periods.



The second graph is for **Login Failures (Bad User Name) per Day**, relatively rare incidents because PAM manages access to the network, but it can be valuable to know when and how often such activity occurs.

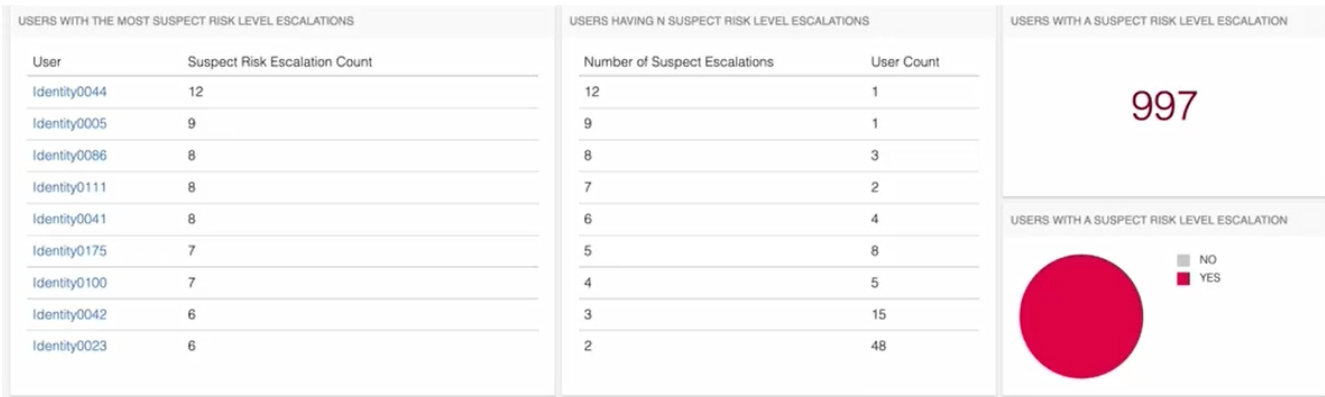
### **Risk: How Risky Are my Users?**

The **Risk** section of the **Data Insights** page provides counts of users with and without new risk level escalations and the number of users with both **Bad** and **Suspect** risk-level escalations. Pie charts help highlight the percentage of risky users on the network.



The **Risk** section also lists users with the following characteristics:

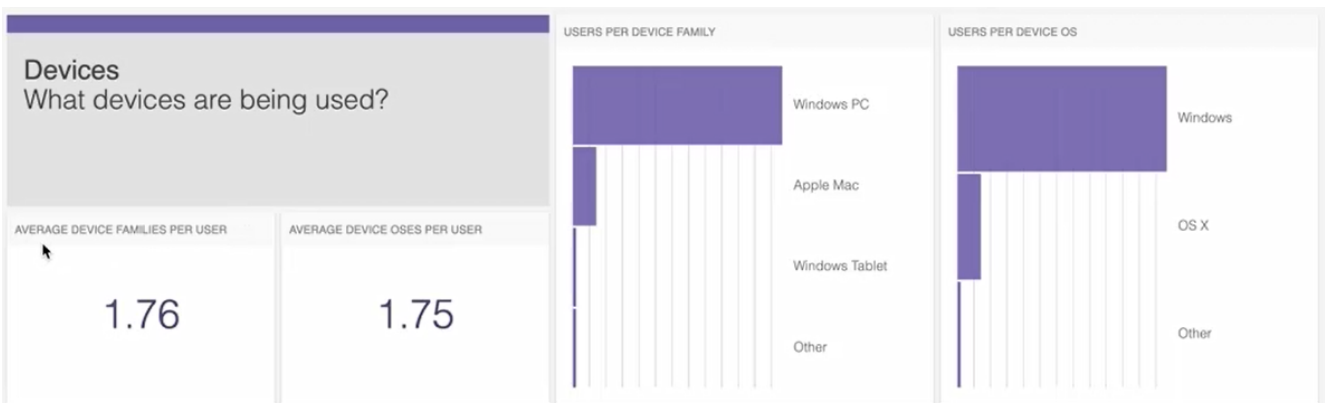
- The most suspect risk level activity escalations
- The number of suspect escalations
- The user count
- The count of users with a suspect risk level escalation
- A pie chart of users with a suspect risk level escalation



### Devices: Which Devices Are Being Used?

The **Devices** section provides the following information:

- The average number of device families and device operating systems per user
- A bar chart of users per device family
- A bar chart of users per device operating systems



## Track Risk Level Activity for All Users and Devices

The **Risk Level Activity** panel that was described earlier can be a useful tool to explore all kinds of risky behavior that is linked to users, devices, activities, analytics, locations, IP sessions, service users, service sessions, resources, and logs. From this one screen, you can examine all phases of risky network activity on your network. The **Risk Level Activity** panel has two separate sets of menus, one for users (with 10 submenus) and one for devices (with seven submenus).

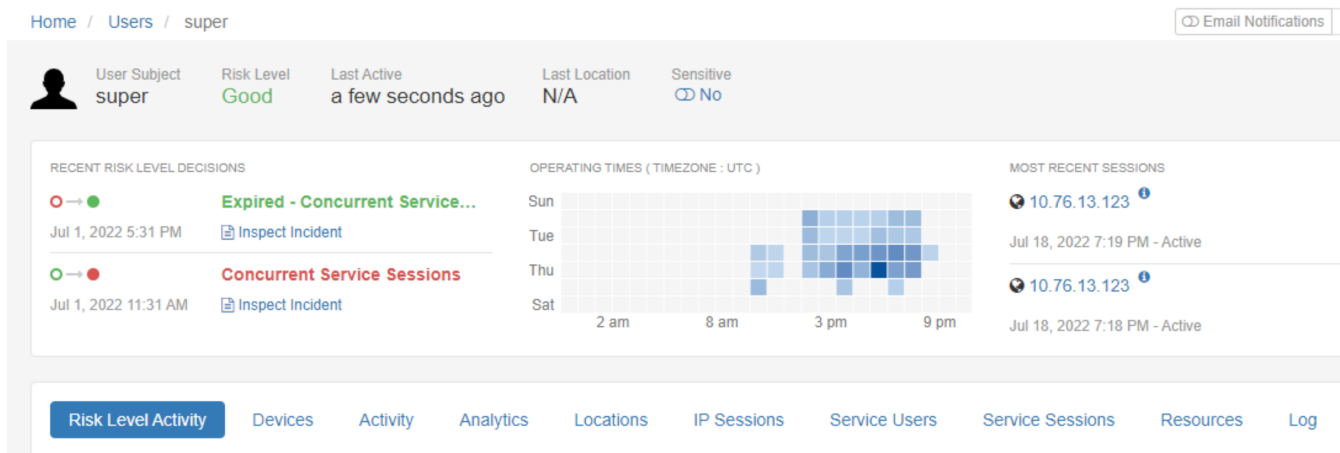
### View a Summary of User and Device Risk Level Activity

Typically users enter the **Risk Level Activity** panel by selecting a user or device. The label at the top of the screen provides the following features:

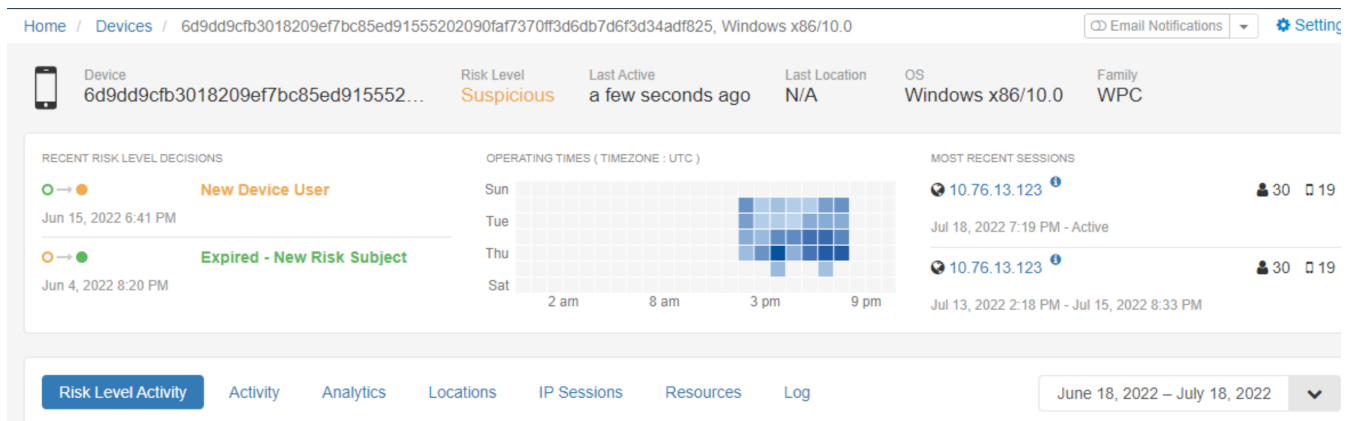
- A list of the most recently triggered analytics
- A heat map over a specified period of operating times
- The IP address and connection method for the most recent sessions
- The dates and times of those sessions

The view then scrolls down to the line of menus. This user or device header remains above the timeline, readily accessible at any time as you open each submenu.

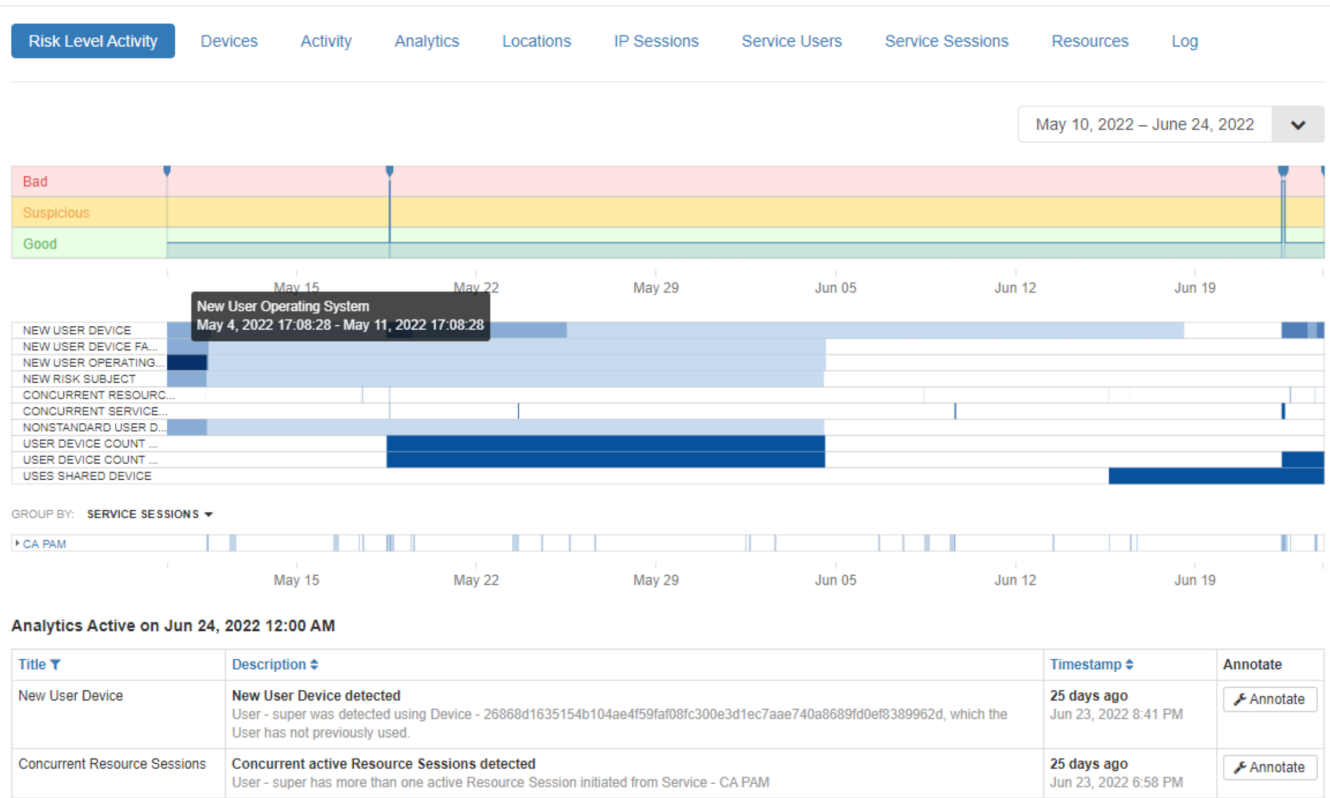
The **Risk Level Activity** header for a user appears similar to the following graphic:



The **Risk Level Activity** header for a device appears similar to the following graphic:

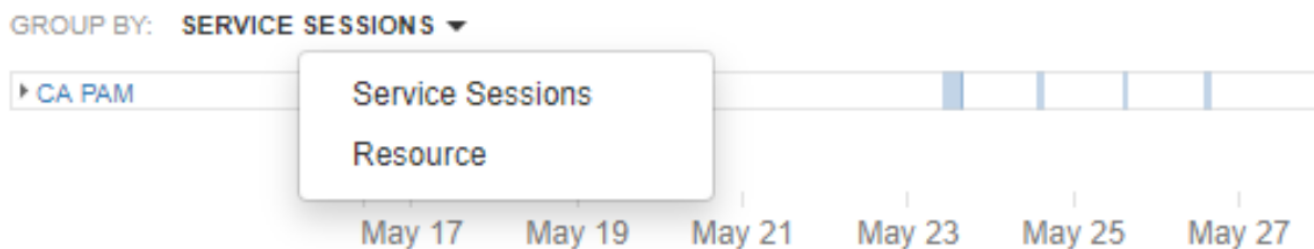


A bar-graph time line of risk level activities starts below the row of menu tabs, along with heat maps similar to the **Overview** screen. The active analytics appear below the heat maps. The timeline has three zones that record **Normal**, **Suspicious**, and **Bad** activity and vertical lines show when a triggered analytic appears on the timeline.

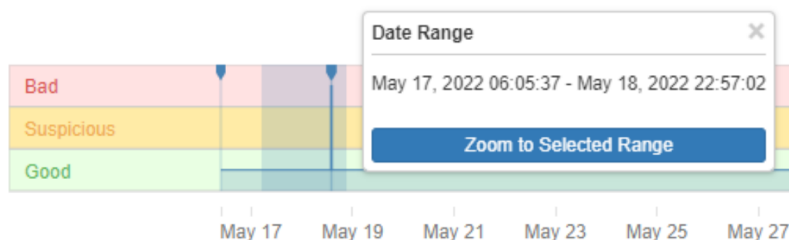


The three bands in the time line bar graph help you determine when and how long an analytic was active, and when it became **Suspicious** or **Bad**, or when it returned to **Normal**.

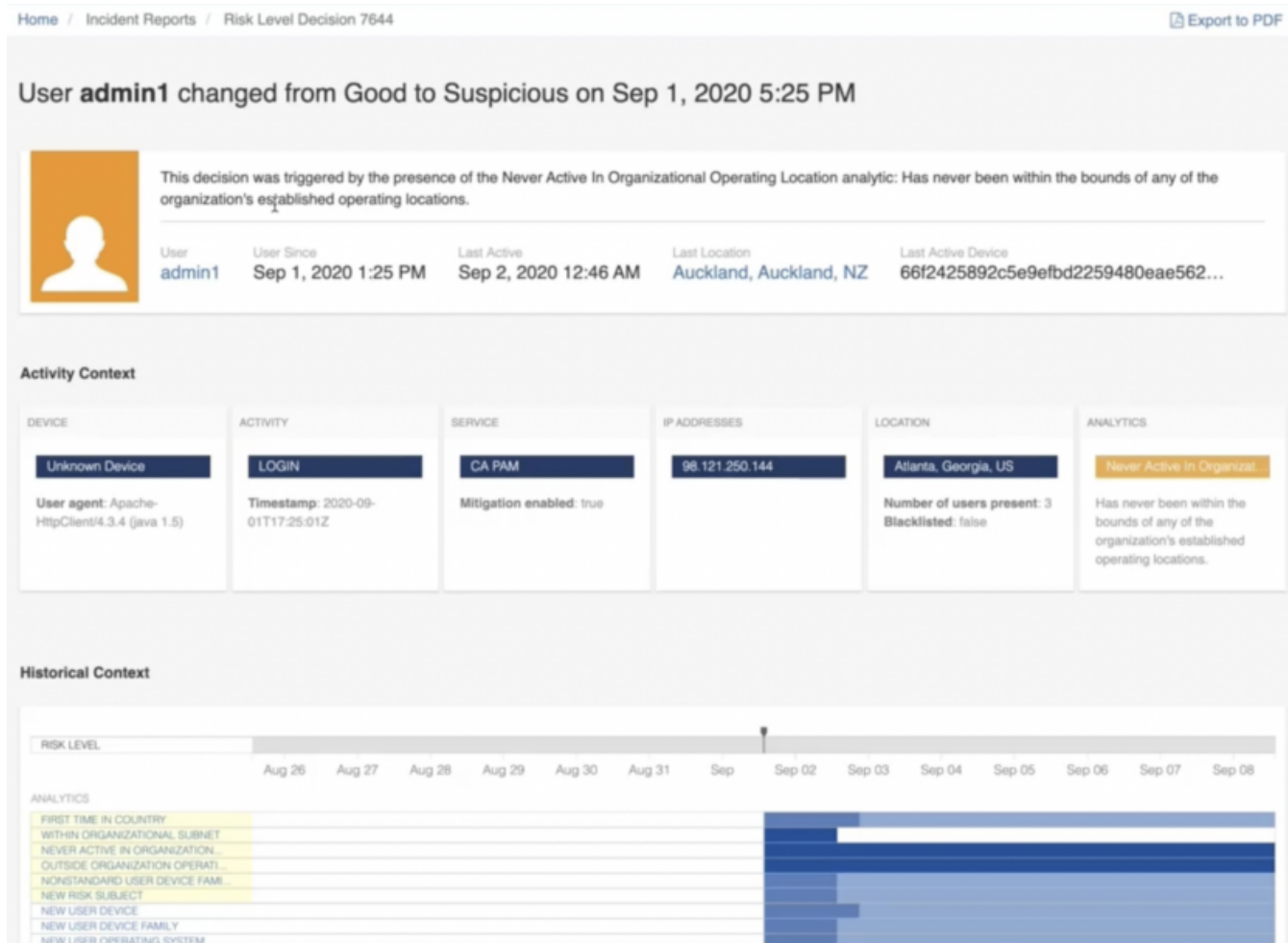
A one-line heat map of all service sessions or resources appears below the heat map. You can select the “Group By” entry to toggle between service sessions and resources.



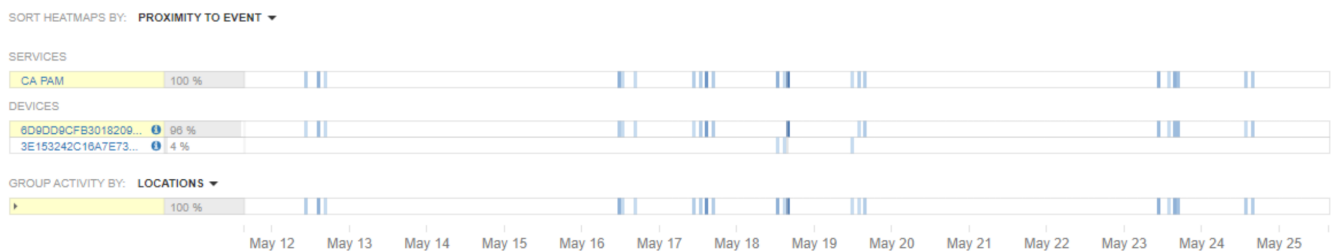
You can drag the cursor through portions of the bar graph to isolate a portion of the graph. If you select the “Zoom to Selected Range” button, only the activity in the selected range displays on the time line and heat map.



Selecting the “Inspect Incident” links right below each analytic message in the **Recent Risk Level Decisions** list of the user header displays more details about the risk level changes and a heat map of previous problematic analytics is generated.



The risk level graph pane also shows separate heat maps for the services, devices, and locations used in the past.



A comprehensive activity log similar to the following one appears after the heat maps:

## Activity Log

Timestamp (UTC)	Device	Action - Resource	IP	Location	Client
May 12, 2022 6:47 PM	6d9dd9cfb3018209ef7bc...	SSO - tap.ca.com	10.76.13.123		Java
May 12, 2022 8:31 PM	6d9dd9cfb3018209ef7bc...	LOGOUT - CA PAM	10.76.13.123		Java
May 16, 2022 3:07 PM	Windows PC (Personal ...)	LOGIN - CA PAM	10.76.13.123		Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
May 16, 2022 3:18 PM	6d9dd9cfb3018209ef7bc...	SSO - tap.ca.com	10.76.13.123		Java
May 16, 2022 3:54 PM	6d9dd9cfb3018209ef7bc...	LOGOUT - CA PAM	10.76.13.123		Java

The links to the devices, resources, and IPs used are all active, so that every detail can be investigated more deeply.

### Get More Details about Risk Level Activity

All the **Risk Level Activity** menu tabs retain the same user or device header section. The **Devices** menu tab takes you to a list of devices used with the operating systems, the latest risk level decisions and locations, and the status of all four categories of analytics. This display is similar to what the **Devices** menu on the top row of the main window generates, but also includes an extra list of “device templates” with their respective operating systems and clients.

[Risk Level Activity](#)
[Devices](#)
[Activity](#)
[Analytics](#)
[Locations](#)
[IP Sessions](#)
[Service Users](#)
[Service Sessions](#)
[Resources](#)
[Log](#)

## ACTIVE DEVICES

Title	OS	Latest Risk Level Decision	Latest Location	Location	Integrity	Activity	Sensitivity
239e1ab7a0c1488e64... Dominant	Windows x64/6.3	Expired - New Risk Subject New Device Jun 4, 2022 8:55 PM	Active for a day starting May 4, 2022				
3e153242c16a7e7368... Dominant	Windows x86/10.0	New Risk Subject New Device May 18, 2022 4:55 PM	Active for 2 days starting May 18, 2022				
6d9dd9cfb3018209ef7... Dominant	Windows x86/10.0	New Device User New Device User detected Jun 15, 2022 6:41 PM	Active for 21 hours starting Jun 15, 2022				
890ea5626a08013db2... Dominant	Windows x86/10.0	Expired - New Risk Subject New Device Jun 4, 2022 8:50 PM	Active for a day starting May 4, 2022				
ae21e73862178c4d3a... Dominant	Windows x86/10.0	Expired - New Risk Subject New Device Jun 4, 2022 7:10 PM	Active for 2 days starting May 4, 2022				
e4ad405c1ee6e0a4e8... Dominant	Windows x86/10.0	Expired - New Risk Subject New Device Jun 4, 2022 5:10 PM	Active for a day starting May 4, 2022				

## DEVICE TEMPLATES

Title	OS	Client
Apple Mac (Personal Computer) running OS X 10.15	OS X 10.15	Firefox 99.0 Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:99.0) Gecko/20100101 Firefox/99.0
Other (Other) running Other 1.8.0_322	Other 1.8.0_322	Other Library 4.5.13 Apache-HttpClient/4.5.13 (Java/1.8.0_322)
Windows PC (Personal Computer) running Windows 10.0	Windows 10.0	Chrome 101.0.4951.41 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

The **Activity** menu tab on the **Risk Level Activity** panel shows the same table as the **Activity** tab on the **Overview** home page. The **Locations** tab also duplicates the **Location** menu on the **Overview** panel.

The **IP Sessions** tab produces the following details:

- A location map
- A table with the city or region
- The session start and end times
- The connection type
- Users sessions
- Devices sessions

You can specify the start and end dates for the data to display. This particular data view is not duplicated anywhere else on the Threat Analytics console.



ANIMATE LOCATIONS

⏮ ⏪ ⏩ ⏭ TIME Hour Day Week Month

START: DEC 16, 2021 4:05 PM – END: DEC 23, 2021 4:05 PM

IP Address	City, Region	Session start	Session end	Connection Type	Users sessions	Devices sessions
10.76.13.123 ⓘ Active for a day since Jun 15, 2022 6:21 PM	N/A	Jun 15, 2022 6:21 PM	Active	N/A	17	10
10.76.13.123 ⓘ Active for a day since Jun 15, 2022 6:20 PM	N/A	Jun 15, 2022 6:20 PM	Active	N/A	17	
10.76.13.123 ⓘ Active for a day - expired on Jun 14, 2022 2:30 PM	N/A	Jun 13, 2022 2:26 PM	Jun 14, 2022 2:30 PM	N/A	17	10
10.76.13.123 ⓘ Active for a day - expired on Jun 14, 2022 2:29 PM	N/A	Jun 13, 2022 2:21 PM	Jun 14, 2022 2:29 PM	N/A	17	

The **Service Users** tab lists the services that are used by each user on the network.

Risk Level Activity Devices Activity Analytics Locations IP Sessions **Service Users** Service Sessions Resources Log

Title	Identifier	Service	Active
super	1	CA PAM	✓

The **Service Sessions** tab lists the following information for each entry:

- The service used
- The user involved
- A link to more details about the service session
- The start and end times of each session
- The duration of the session
- The resource session count



Risk Level Activity   Devices   Activity   Analytics   Locations   IP Sessions   Service Users   **Service Sessions**   Resources   Log

June 21, 2022 – July 21, 2022

Service	User	Service Session	Session Start	Session End	Session Duration	Resource Sessions Count
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 21, 2022 7:38 PM	Active	38 Sec	2
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 20, 2022 7:06 PM	Jul 20, 2022 7:51 PM	2682 Sec	4
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 20, 2022 6:14 PM	Jul 20, 2022 7:01 PM	2832 Sec	1
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 20, 2022 3:04 PM	Jul 20, 2022 4:06 PM	3689 Sec	1
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 19, 2022 7:33 PM	Jul 19, 2022 8:32 PM	3557 Sec	1
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 18, 2022 7:18 PM	Jul 18, 2022 8:40 PM	4878 Sec	1
CA PAM	super ⓘ	<a href="#">Session Details ⓘ</a>	Jul 14, 2022 6:05 PM	Jul 14, 2022 8:33 PM	8901 Sec	4

This Resource Session Count pane is the same one that is shown by the **Services** menu at the top of the main screen when you select a specific service (in this case, CA Privileged Access Manager) and then select the **Service Sessions** menu.

The **Resources** tab lists the resources that are used by the service and their identifiers. The **Resources** tab is similar to the **Resources** menu at the top of the main screen.

Risk Level Activity   Devices   Activity   Analytics   Locations   IP Sessions   Service Users   **Service Sessions**   **Resources**   Log

Service	Title	Identifier	Sensitive
CA PAM	<a href="#">CA PAM ⓘ</a>	74a0acb7-66d7-4178-942d-d355b8f04243	
CA PAM	<a href="#">tap.ca.com ⓘ</a>	22001	

The **Log** tab provides a table of timestamps, event types, and a description of each log. You can select the blue “Download as .csv” text in the top row to save a copy of the log list.

<a href="#">Download as .csv</a>		
Timestamp	Type	Description
Jun 16, 2022 2:25 PM	Risk Factor Decision	User - super had its Activity Risk Factor changed from Good to Suspect
Jun 16, 2022 2:25 PM	Analytic Decision	Analytic - Concurrent Resource Sessions triggered for User - super. User - super has more than one active Resource Session initiated from Service - CA PAM
Jun 15, 2022 6:41 PM	Analytic Decision	Analytic - Uses Shared Device triggered for User - super. User - super is associated with Device - 6d9dd9cfb3018209ef7bc85ed91555202090fa7370ff3d6db7d6f3d34ad825, which is shared by multiple Users - super, Bob Lee
Jun 15, 2022 6:27 PM	Risk Factor Decision	User - super had its Activity Risk Factor changed from Suspect to Good
Jun 15, 2022 6:27 PM	Analytic Decision	Analytic - Concurrent Resource Sessions expired for User - super. User - super has more than one active Resource Session initiated from Service - CA PAM
Jun 15, 2022 6:21 PM	Risk Factor Decision	User - super had its Activity Risk Factor changed from Good to Suspect
Jun 15, 2022 6:21 PM	Analytic Decision	Analytic - Concurrent Resource Sessions triggered for User - super. User - super has more than one active Resource Session initiated from Service - CA PAM
Jun 15, 2022 6:21 PM	Ip Session	IP Address - 10.76.13.123 was associated with Device - 6d9dd9cfb3018209ef7bc85ed91555202090fa7370ff3d6db7d6f3d34ad825 and User - super
Jun 15, 2022 6:20 PM	Ip Session	IP Address - 10.76.13.123 was associated with Device - Unknown Device and User - super

## Configure Threat Analytics Console Settings

As a user with administrative privileges, you can configure the properties of the Threat Analytics Console from the **Settings** panel.

### NOTE

If you do not have administrative privileges, see [Enable Admin Privileges for Users](#).

To access the **Settings** panel, select the gear icon at the top-right corner of the console and select **Settings** from the menu that opens.

Use the following tabs on the menu at the top of the **Settings** panel to access controls for configuring corresponding properties of the Threat Analytics Console:

- **User Accounts:** A list of user accounts with administration capabilities and status (see [Manage Threat Analytics Users](#))
- **Device Analytics:** A list of all *device* analytics that allows you to disable or enable each one (see [Select which Device Analytics Are Enabled or Disabled](#))
- **User Analytics:** A list of all user analytics that allows you to disable or enable each one (see [Select which User Analytics Are Enabled or Disabled](#))
- **Locations:** Allow or refuse access based on what country users are operating in (see [Whitelist or Blacklist Users from Network Locations Based on Country](#))
- **Operating Locations:** Map User Locations based on IP Address (see [Manually Identify Device Locations](#))
- **Subnets:** Maintains lists of subnetworks, their individual IP addresses, and their netmasks (see [Manage Subnets](#))
- **SMTP:** Set Up Simple Mail Transfer Protocol for Email (see [Set Up SMTP for Email](#))
- **Syslog:** Set up Syslog and SIEM (see [Configure Syslog/SIEM Logging](#))
- **Advanced:** Create more complex analytic configurations and operations (see [Modify Analytic Configurations, Jobs, and Mixing Functions](#))

## Manage Threat Analytics Users

Select the **User Account** tab from the **Settings** panel menu to open the **Manage User Accounts** pane from which you can do the following tasks:

- Add Threat Analytics user accounts
- Manage existing Threat Analytics accounts (for example, assign administrative privileges, lock, and delete)

[Home](#) / [Settings](#)

Login	Email	Admin	Enabled	Locked	Source	Last Login Time	Last Login IP	Actions
admin	admin@localhost.local	✓	✓		interlock	Jul 1, 2022 11:14 AM	127.0.0.1	<a href="#">Edit</a> <a href="#">Delete</a>
super	super@pam.local	✓	✓		saml	Jul 5, 2022 6:35 PM	127.0.0.1	<a href="#">Edit</a>

### Add a User

Complete this procedure to create a Threat Analytics user account.

#### Follow these steps:

1. Select the **+ Add User** button. The **Create User** pane opens.
2. Complete the following fields and options, as required:

- **Login:** The login name of the new user.
- **Email:** The email address of the new user
- **Password:** The password for the new user; this password is evaluated and if accepted a green “Strong Password” message appears.
- **Confirm Password:** Enter the same password to verify all characters
- **Enabled:** Set this option to enable the user account.
- **Admin:** Set this option to assign administrative privileges to the user account
- **SMTP Settings:** (Informational)  
Shows the current SMTP status (whether email is enabled or disabled). To change the setting, select the
- **Alerts:** Specify the frequency of **System Alerts**, **Service Alerts**, and **Risk Escalation Alerts** by selecting one of the following values from the associated drop-down menu:
  - **Inactive**
  - **Immediately**
  - **Hourly**
  - **Daily**
  - **Weekly**

3. Select the **Save** button. The user is created and added to the user account table.

### **Manage Existing Users**

The user account table displays static and manageable properties of existing users and allows you to:

- **Login:** The login name of the user.
- **Email:** The email address of the user.
- **Admin:** Specifies whether the user has administrative privileges. If yes, a checkmark icon is present. If no, an empty checkbox is present. Select the checkmark icon or checkbox to toggle the setting.
- **Enabled:** Specifies whether the user is enabled. If yes, a checkmark icon is present. If no, an empty checkbox is present. Select the checkmark icon or checkbox to toggle the setting.
- **Locked:** Specifies whether the user account is locked out. If yes, a checkmark icon is present. If no, an empty checkbox is present. Select the checkmark icon or checkbox to toggle the setting.
- **Source:** The access method of the user (for example, SAML)
- **Last Login Time:** The last time the user logged in.
- **Last Login IP:** The IP address from which the user logged in.
- **Actions:** Provides the following options:
  - **Edit:** Open the account for editing in the **Edit User** pane (which is similar to the **Create User** pane).
  - **Delete:** Delete the user account.

## **Select which Device Analytics Are Enabled or Disabled**

Access the **Device Analytics** tab from the **Settings** panel menu to enable or disable any of the 58 available risk level analytics for all *devices* on the network. All analytics are enabled by default.

In the following example, the "Bad Associated Risk Subject" and "Crossed Organizational Subnet Boundary" options are not set. Those analytics are therefore disabled for all devices.

User Accounts
Device Analytics
User Analytics
Locations
Operating Locations
Subnets
SMTP
Syslog
Advanced

### Specify Which Analytics Contribute To Risk Level

<input checked="" type="checkbox"/>	Abnormal Resource Session Rate	is contributing
<input checked="" type="checkbox"/>	Abnormal Resource Session Rate for User Subject	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Resource Session	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Resource Session For User Subject	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Service Session	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Service Session for Identity	is contributing
<input checked="" type="checkbox"/>	Access Denials	is contributing
<input checked="" type="checkbox"/>	Accessing Sensitive Resource	is contributing
<input checked="" type="checkbox"/>	Associated With Deactivated User	is contributing
<input type="checkbox"/>	Bad Associated Risk Subject	is <b>NOT</b> contributing
<input checked="" type="checkbox"/>	Blacklisted Location	is contributing
<input checked="" type="checkbox"/>	Changed Countries	is contributing
<input checked="" type="checkbox"/>	Concurrent Resource Sessions	is contributing
<input checked="" type="checkbox"/>	Concurrent Service Sessions	is contributing
<input type="checkbox"/>	Crossed Organizational Subnet Boundary	is <b>NOT</b> contributing
<input checked="" type="checkbox"/>	Data Downloaded	is contributing
<input checked="" type="checkbox"/>	Distance Travelled	is contributing

## Select which User Analytics Are Enabled or Disabled

Access the **User Analytics** tab from the **Settings** panel menu to enable or disable any of the 58 available risk level analytics for all *users* on the network. All analytics are enabled by default.

In the following example, the "Bad Associated Risk Subject" and "Crossed Organizational Subnet Boundary" options are not set. Those analytics are therefore disabled for all users.

User Accounts
Device Analytics
**User Analytics**
Locations
Operating Locations
Subnets
SMTP
Syslog
Advanced

### Specify Which Analytics Contribute To Risk Level

<input checked="" type="checkbox"/>	Abnormal Resource Session Rate	is contributing
<input checked="" type="checkbox"/>	Abnormal Resource Session Rate for User Subject	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Resource Session	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Resource Session For User Subject	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Service Session	is contributing
<input checked="" type="checkbox"/>	Abnormally Long Service Session for Identity	is contributing
<input checked="" type="checkbox"/>	Access Denials	is contributing
<input checked="" type="checkbox"/>	Accessing Sensitive Resource	is contributing
<input checked="" type="checkbox"/>	Associated With Deactivated User	is contributing
<input type="checkbox"/>	Bad Associated Risk Subject	is <b>NOT</b> contributing Updated 4 minutes ago
<input checked="" type="checkbox"/>	Blacklisted Location	is contributing
<input type="checkbox"/>	Changed Countries	is <b>NOT</b> contributing Updated 4 minutes ago
<input checked="" type="checkbox"/>	Concurrent Resource Sessions	is contributing
<input checked="" type="checkbox"/>	Concurrent Service Sessions	is contributing
<input type="checkbox"/>	Crossed Organizational Subnet Boundary	is <b>NOT</b> contributing Updated 4 minutes ago

## Whitelist or Blacklist Users from Network Locations Based on Country

Select the **Locations** tab from the **Settings** panel to allow or refuse network access to all users based on the country in which they are located using a *whitelist* **or** a *blacklist*.

A whitelist explicitly specifies the countries from which use users *are* accepted on the network. A blacklist explicitly specifies the countries from which users are *not* accepted on the network. (Whitelists and blacklists are therefore mutually exclusive.)

Use the **Whitelist** tab to configure a whitelist. Select the **Blacklist** tab to configure a blacklist. Both tabs are similar, each displaying a list of countries in alphabetical order and a **Search** field to quickly locate a specific country.

### Configure a Whitelist

Use this procedure to configure a whitelist.

#### Follow these steps:

1. Select the **Whitelist** tab.
2. Do the following steps to *add* a country to the whitelist:
  - a. Select the target country by scrolling down the list of locations on the left or by using the **Search** field.
  - b. Select the **Add** button in the **Action** column. The country is added to the list of **Whitelisted Locations** on the right.
3. To remove a country from the whitelist, select the red **Remove** button beside the list of **Whitelisted Locations** on the right.

### Configure a Blacklist

Use this procedure to configure a blacklist.

**Follow these steps:**

1. Select the **Blacklist** tab.
2. Do the following steps to *add* a country to the blacklist:
  - a. Select the target country by scrolling down the list of locations on the left or by using the **Search** field.
  - b. Select the **Add** button in the **Action** column. The country is added to the list of **Blacklisted Locations** on the right.
3. To remove a country from the blacklist, select the red **Remove** button beside the list of **Whitelisted Locations** on the right.

## Manually Identify Device Locations

If the physical location of a site cannot be determined from its IP address, you can manually identify its location using one of the following techniques:

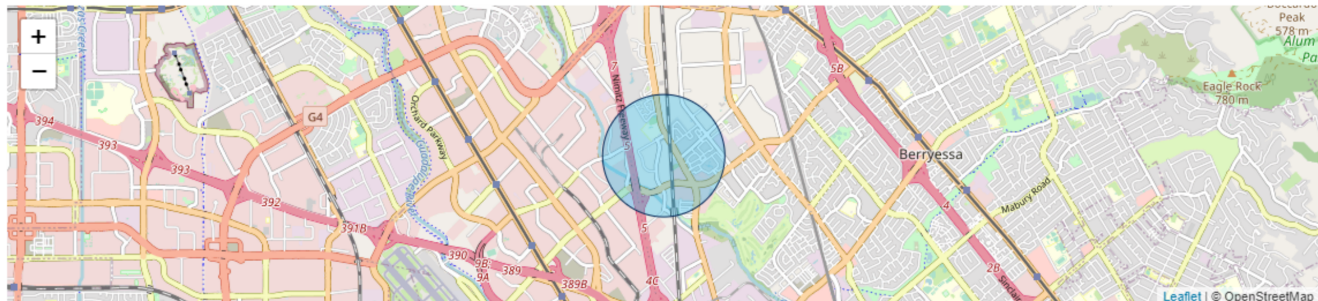
- Specify the coordinates of the site using its latitude and longitude
- Navigate to the site location using the map

**Follow these steps:**

1. Select the **Operating Locations** tab from the **Settings** panel. The **Managing Operating Locations** pane opens as shown in the following example:

User Accounts   Device Analytics   User Analytics   Locations   **Operating Locations**   Subnets   SMTP   Syslog   Advanced

### Manage Operating Locations



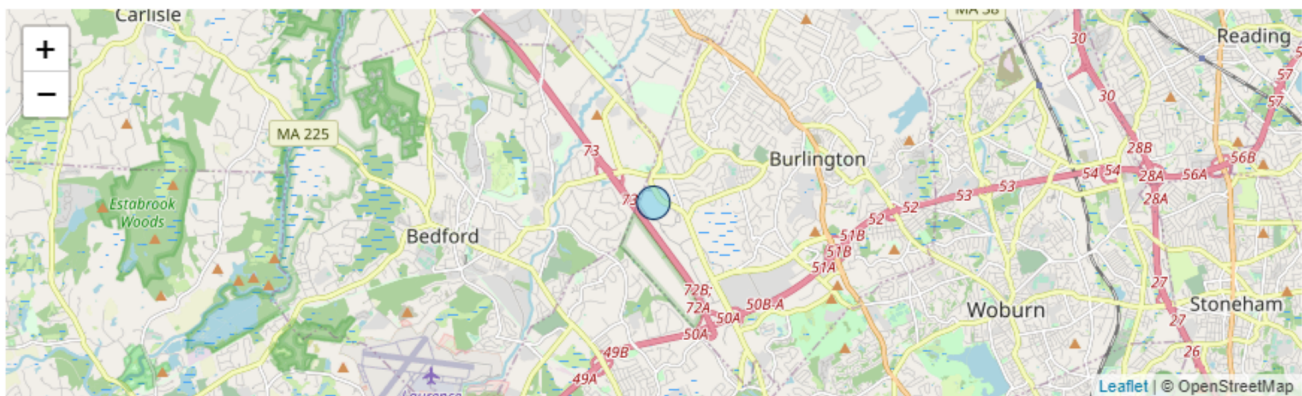
**+ Add Operating Location**

Title	Timezone	Radius (miles)	Created	Actions
Operating location at 37.3861, -121.9003 <a href="#">Focus Map</a>		1 mi	Jul 11, 2022 4:10 PM	<a href="#">Delete</a>

2. Select the **Add Operating Location** button. The **Add Operating Location** pane opens as shown in the following example:



## Add Operating Location



Click to add a point. Click the point to change the radius. Click the map to release the radius.

✖ Clear Map

Latitude	Longitude	Radius (miles)	
42.49728891992472	-71.23337745666505	0.2	<a href="#">+ Add Location</a>

### 3. Do one of the following actions:

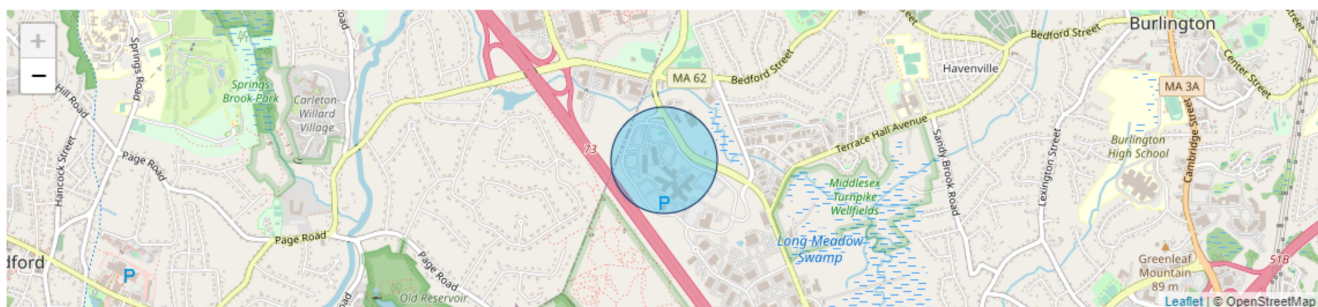
- Enter the site coordinates in the **Latitude** and **Longitude** fields. Use positive coordinates for northern latitudes and eastern longitudes and use negative coordinates for southern latitudes and western longitudes.
- Manipulate the map until the site location is centered.

### 4. Enter the margin of error for the site location in the **Radius** field.

The location that you entered is added to the operating locations list. The **Focus Map** text under each operating location takes you to a view of that particular location, as shown in the following example:

[User Accounts](#) [Device Analytics](#) [User Analytics](#) [Locations](#) [Operating Locations](#) [Subnets](#) [SMTP](#) [Syslog](#) [Advanced](#)

## Manage Operating Locations



[+ Add Operating Location](#)

Title	Timezone	Radius (miles)	Created	Actions
Operating location at 37.3861, -121.9003 <a href="#">Focus Map</a>		1 mi	Jul 11, 2022 4:10 PM	<a href="#">Delete</a>
Operating location at 42.49728891992473, -71.23337745666504 <a href="#">Focus Map</a>		0 mi	Jul 11, 2022 3:55 PM	<a href="#">Delete</a>

To delete a site, select the **Delete** button in the **Action** column of its entry in the operating locations list.

## Manage Subnets

A subnet is a segmented piece of a larger network, partitioned into multiple smaller network segments to help minimize the traffic. This segmenting splits a large network into groups of smaller interconnected networks, increasing transmission speeds.

To view and add subnets, select the **Subnets** tab from the **Settings** panel. The **Manage Subnets** pane that opens displays a list of each active subnet together with the following associated properties:

- **Title** (a numerical value)
- **IP Address**
- **Netmask** address
- The date and time that it was **Created**
- Whether the subnet is **Suspicious**
- Whether the subnet is part of the **Organization**
- The **Subnet Group** category of each subnet. (One of Amazon Web Services (AWS), RSLynx (RS), Google, or WA).

The following screenshot shows an example **Manage Subnets** pane.



User Accounts

Device Analytics

User Analytics

Locations

Operating Locations

Subnets

SMTP

## Manage Subnets

Search by:


☒ Title☐ IP Address

Subnets Title

Search

Clear

[+ Add Subnet](#)

Title	IP Address	Netmask	Created	Suspicious 	Organizat
Subnet 23.20.0.0/14	23.20.0.0	255.252.0.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.0.0/18	23.96.0.0	255.255.192.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.64.0/28	23.96.64.0	255.255.255.240	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.64.64/26	23.96.64.64	255.255.255.192	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.64.128/27	23.96.64.128	255.255.255.224	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.64.160/28	23.96.64.160	255.255.255.240	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.80.0/20	23.96.80.0	255.255.240.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.96.0/19	23.96.96.0	255.255.224.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.128.0/18	23.96.128.0	255.255.192.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.96.192.0/19	23.96.192.0	255.255.224.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.97.48.0/20	23.97.48.0	255.255.240.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.97.64.0/20	23.97.64.0	255.255.240.0	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Subnet 23.97.80.0/28	23.97.80.0	255.255.255.240	Oct 18, 2016 8:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>

To add a subnet, select the **Add Subnet** button and supply the required properties.

### NOTE

You cannot delete a subnet from the Threat Analytics Console.

## Set Up SMTP for Email

Simple Mail Transfer Protocol (SMTP), is an email protocol for sending emails between clients and accounts. To manage SMTP settings, select the **SMTP** tab from the **Settings** panel menu.

To configure the SMTP settings for Threat Analytics, configure the following settings as appropriate:

- **Enable System Emails:** Set this option to enable system emails.
- **Default From Address:** Specifies the email address of the user account from which messages are sent. Select the **Save** button to save the address. Select the **Send Test Mail** button to send a test message.
- **Host:** The host address to use.
- **Port Number:** The port number to use.
- **Domain:** The domain to use.
- **Use SSL :** Set this option to use SSL.
- **Authentication** (Optional): Specify the type of authentication to use; the options are Plain, Login, and CRAM-MD5. If an authentication method is specified, the following fields appear:
  - **Username:** The username of the account to use for authentication.
  - **Password:** The password of the account to use for authentication.

Select the **Save** button to commit your changes.

The following screenshot shows an example of a typical configuration:

User Accounts Device Analytics User Analytics Locations Operating Locations Subnets **SMTP** Syslog Advanced

### Manage SMTP Settings For Email Notifications

Enable System Emails ☒

Default From Address administrator@forwardinc.ca

✓ Save ↗ Send Test Email

Host Host

Port Number Port

Domain Domain

Use SSL ☐

Authentication --- ▼

✓ Save

## Configure Syslog/SIEM Logging

Syslog is a message logging protocol that handles the event data management and security. Syslog also monitors informational, analysis, and debugging messages. Syslog is essentially a mechanism for network devices to send event messages to a logging server, but it provides no analysis of the log data.

SIEM ([Security Information and Event Management](#)) goes further, combining event logs with contextual information about users and their vulnerabilities. SIEM also uses algorithms, rules, and statistics to compare the devices.

You configure Syslog and SIEM logging from the **Syslog** tab on the **Settings** panel menu.

### **Configure Syslog/SIEM Server Definitions**

Do this procedure to configure Syslog/SIEM server definitions.

**Follow these steps for each Syslog/SIEM server that you want to configure:**

1. Select the **Create Server Config** button.
2. Complete the following fields:
  - **IP**: The server IP address.
  - **Port**: The server port number.
  - **Protocol**: The server communication protocol (TCP or UDP).
3. Select the **Save** button to commit your changes.

The new server definition is listed at the top of the pane, as shown in the following screenshot:

IP	Port	Protocol	Created At	Actions
10.17.40.159	25	tcp	Jul 13, 2022 2:56 PM	<a href="#">Edit</a> <a href="#">Delete</a>

Alert me on: Risk Level Changes Transition: All Changes

[Save Filter Config](#)

**To edit a server definition:** Select the **Edit** button in the **Actions** column of the corresponding entry in the server list.

**To remove a server definition:** Select the **Delete** button in the **Actions** column of the corresponding entry in the server list.

### **Configure Filters to Limit the Events That Trigger an Alert**

By default, all events trigger an alert. This procedure describes how to configure filters that limit the changes that trigger an alert.

**Follow these steps for each filter that you want to create:**

1. Select one of the following options from the **Alert me on** drop-down.

- **All Changes** (Default): All events trigger an alert.
  - **Risk Level Changes**: All risk level changes trigger an alert.
  - **Analytic Triggers**: Only the analytics that you specify in the following step trigger alerts.
2. If you selected **Analytic Triggers**, select one of the following options from the **Transition** drop-down list that appears:
- **All Analytics**
  - **All Location Analytics**
  - **All Activity Analytics**
  - **All Sensitivity Analytics**
  - **All Integrity Analytics**
  - **Specific Analytics**
3. Select the **Save Filter Config** button.

The filter is added to the **Current Syslog/SIEM Filters** list.

**To remove a filter:** Select the **Delete** button in the **Actions** column of the corresponding entry in the filters list.

## Modify Analytic Configurations, Jobs, and Mixing Functions

Select the **Advanced** tab from the **Settings** panel to access the advanced threat analytics configuration options.



### CAUTION

Change these settings with caution, preferably with the assistance of Broadcom Support.

The **Risk Analysis** section lets you modify the threshold for how many possibly suspicious incidents should be shown. This section does not enable or disable individual analytics, but instead specifies whether you want to view more incidents or fewer incidents overall. There is also a **Reset to defaults** button to return to the original settings.

[User Accounts](#)[Device Analytics](#)[User Analytics](#)[Locations](#)[Operating Locations](#)[Subnets](#)[SMTP](#)[Syslog](#)[Advanced](#)

## Advanced

### Risk Analysis

These controls modify how the system evaluates risk. Be cautious about using them! Setting the value too low may cause the system to show no incidents, while setting it too high may generate too many incidents to deal with.

[+ Show me \*\*more\*\* incidents](#)
[- Show me \*\*fewer\*\* incidents](#)
[✕ Reset to defaults](#)

### Analytic Baseline Configurations

Make changes to [analytic baseline values](#).

### Advanced Configuration

Make changes to [advanced configuration values](#).

### Jobs

Administer [Jobs](#).

### Mixing Function

Current [Mixing Function](#) updated **Oct 18, 2016 4:52 PM**

Hash: aa4337cc4e08c36c81fed5b1e16ab4e7

Update Mixing Function  No file chosen

The **Analytic Baseline Configurations** section lets you specify values for five specific analytic keys that govern the number of days with no activity before a user goes dormant, how many devices or device families a user has, how many operating systems associated with, and the number of groups a user can belong to. If a value is not set, the analytic is set to the default value. For example, the “default\_dormant\_days” threshold is 30 days with no activity, but you can make the threshold higher or lower as needed by selecting **Edit**.

#### CA Threat Analytics Configuration

**Warning!** Editing these settings may result in unexpected behavior. Please do not make changes **unless directed to do so by support staff**.

Key	Description	Value	
default_dormant_days Type: Integer	The default number of days with no Activity that must pass before a user is considered Dormant	-- Defaults to 30 when not set	<a href="#">✎ Edit</a>
user_device_count_limit Type: Integer	The hard limit on the number of devices a user can be associated with before being flagged. A value of null indicates no limit.	5 Defaults to Null when not set	<a href="#">✎ Edit</a>
user_device_family_count_limit Type: Integer	The hard limit on the number of device families a user can be associated with before being flagged. A value of null indicates no limit.	3 Defaults to Null when not set	<a href="#">✎ Edit</a>
user_device_os_count_limit Type: Integer	The hard limit on the number of device OSes a user can be associated with before being flagged. A value of null indicates no limit.	3 Defaults to Null when not set	<a href="#">✎ Edit</a>
user_group_count_limit Type: Integer	The hard limit on the number of Groups an identity can belong to before being flagged. A value of null indicates no limit.	-- Defaults to Null when not set	<a href="#">✎ Edit</a>

The **Advanced Configuration Values** section allows you to change the default values for 78 different analytic keys using the **Edit** button. This section is similar to the **Analytic Baseline Configuration** panel.

## CA Threat Analytics Configuration

**Warning!** Editing these settings may result in unexpected behavior. Please do not make changes **unless directed to do so by support staff**.

Key	Description	Value	
api_available Type: Boolean	Is the API Available to process requests? If false, API will return a 503.	-- Defaults to true when not set	<a href="#">Edit</a>
api_documentation_dynamic Type: Boolean	Indicates whether the API Documentation will be dynamically generated	-- Defaults to false when not set	<a href="#">Edit</a>
batch_loading Type: Boolean	Flag indicating whether the system is in a batch loading state, and thus that the jobs should treat time differently.	-- Defaults to false when not set	<a href="#">Edit</a>
cache_data_enabled Type: Boolean	Indicates whether Data/Resources should be cached from remote services, systemwide.	-- Defaults to true when not set	<a href="#">Edit</a>
cache_devices_enabled Type: Boolean	Indicates whether Devices should be cached from remote services, systemwide.	-- Defaults to true	<a href="#">Edit</a>
cache_group_subjects_enabled Type: Boolean	Indicates whether GroupSubjects should be cached from remote services, systemwide.	-- Defaults to true	<a href="#">Edit</a>
cache_ip_mappings_enabled Type: Boolean	Indicates whether IpMappings should be cached from remote services, systemwide.	-- Defaults to true when not set	<a href="#">Edit</a>
cache_user_subject_mappings_enabled Type: Boolean	Indicates whether UserSubjectMappings should be cached from remote services, systemwide.	-- Defaults to true when not set	<a href="#">Edit</a>
cache_user_subjects_enabled Type: Boolean	Indicates whether UserSubjects should be cached from remote services, systemwide.	-- Defaults to true when not set	<a href="#">Edit</a>
default_dormant_days Type: Integer	The default number of days with no Activity that must pass before a user is considered Dormant	-- Defaults to 30 when not set	<a href="#">Edit</a>
demo_mode Type: Boolean	Flag indicating whether the system is in demo mode.	-- Defaults to false when not set	<a href="#">Edit</a>
demo_user_id Type: String		-- Defaults to when not set	<a href="#">Edit</a>

The **Jobs** link on the **Advanced** tab shows the status of the thirty tasks being monitored by the network, presented in alphabetical order.

## CA Threat Analytics Jobs

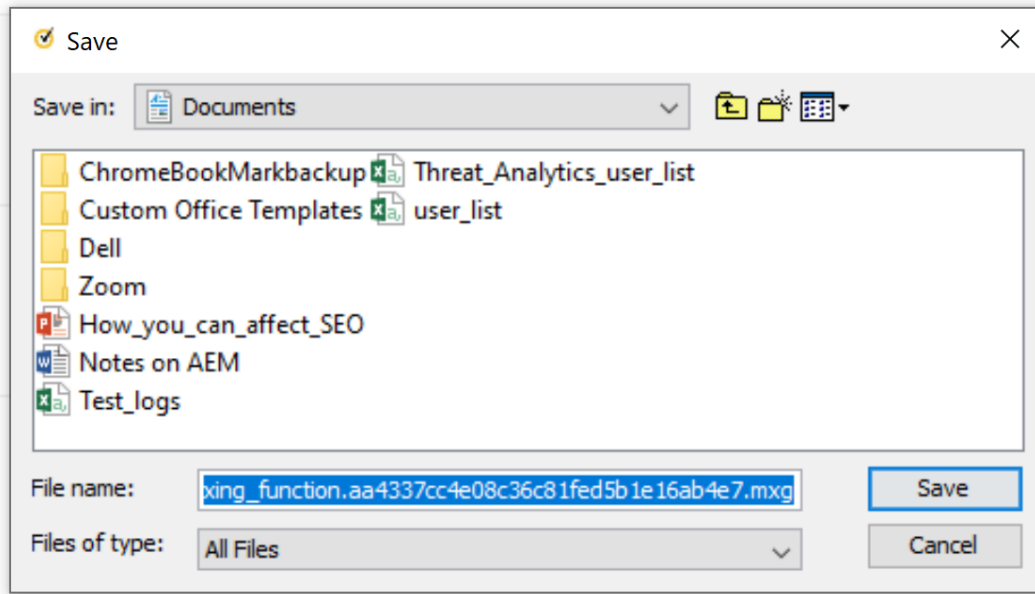
**Warning!** Manually manipulating Jobs may result in unexpected behavior. Please do not make changes **unless directed to do so by support staff**.

Title	Job Name	Enabled	Status	Cron	Timeout	Last Start	Last End	Action
Activity Rollup Job	activity_rollup_job.job	✓	STARTED	0 0 0 * * ?	0s	Jul 13, 2022 12:00 AM	Jul 13, 2022 12:00 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Alert Summarizer	alert_summarizer.job	✓	STARTED	0 0 * * * ?	0s	Jul 13, 2022 6:00 PM	Jul 13, 2022 6:00 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Data Truncator Job	data_truncator_job.job	✓	STARTED	0 0 0 * * ?	0s	Jul 13, 2022 12:00 AM	Jul 13, 2022 12:00 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Database Vacuum Job	database_vacuum_job.job	✓	STARTED	0 30 1 * * ?	0s	Jul 13, 2022 1:30 AM	Jul 13, 2022 1:30 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Decision Watcher	decision_watcher.job	✓	STARTED	0 */5 * * * ?	0s	Jul 13, 2022 6:20 PM	Jul 13, 2022 6:20 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Dormant Risk Subject Watcher	dormant_risk_subject_watcher.job	✓	STARTED	0 0 * * * ?	0s	Jul 13, 2022 6:00 PM	Jul 13, 2022 6:00 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Factoid Calculator Job	factoid_calculator_job.job	✓	STARTED	0 0 2 * * ?	0s	Jul 13, 2022 2:00 AM	Jul 13, 2022 2:00 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Flapping Watcher	flapping_watcher.job	✓	STARTED	0,30 * * * * ?	0s	Jul 13, 2022 6:22 PM	Jul 13, 2022 6:22 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Interlock System Watcher Job	interlock_system_watcher_job.job	✓	STARTED	0 */2 * * * ?	0s	Jul 13, 2022 6:22 PM	Jul 13, 2022 6:22 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Monitor Api Error Rate Job	monitor_api_error_rate_job.job	✓	STARTED	0 */10 * * * ?	0s	Jul 13, 2022 6:20 PM	Jul 13, 2022 6:20 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Monitor Api Rate Job	monitor_api_rate_job.job	✓	STARTED	0 * * * * ?	0s	Jul 13, 2022 6:22 PM	Jul 13, 2022 6:22 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Monitor Performance Job	monitor_performance_job.job	✓	STARTED	0 */10 0 * * ?	0s	Jul 13, 2022 12:50 AM	Jul 13, 2022 12:50 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Monitor Queues Job	monitor_queues_job.job	✓	STARTED	0 * * * * ?	0s	Jul 13, 2022 6:22 PM	Jul 13, 2022 6:22 PM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Numerical Feature Set Job	numerical_feature_set_job.job	✓	STARTED	0 0 4 * * ?	0s	Jul 13, 2022 4:00 AM	Jul 13, 2022 4:00 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Operating Location Calculator	operating_location_calculator.job	✓	STARTED	0 30 3 * * ?	0s	Jul 13, 2022 3:30 AM	Jul 13, 2022 3:30 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>
Operating Times Calculator	operating_times_calculator.job	✓	STARTED	0 0 1 * * ?	0s	Jul 13, 2022 1:00 AM	Jul 13, 2022 1:00 AM	<a href="#">○ Stop</a> <a href="#">⚙ Run</a>

The **Jobs** link provides the following information:

- The job title
- The name of the \*.job file
- Whether it has been enabled
- Its status
- The statistics for a scheduled job or task in UNIX, known as a "cron" job
- How long it has been timed out (when applicable)
- The last start and end times (where relevant)
- Two **Stop** and **Run** buttons to stop or restart the job as needed

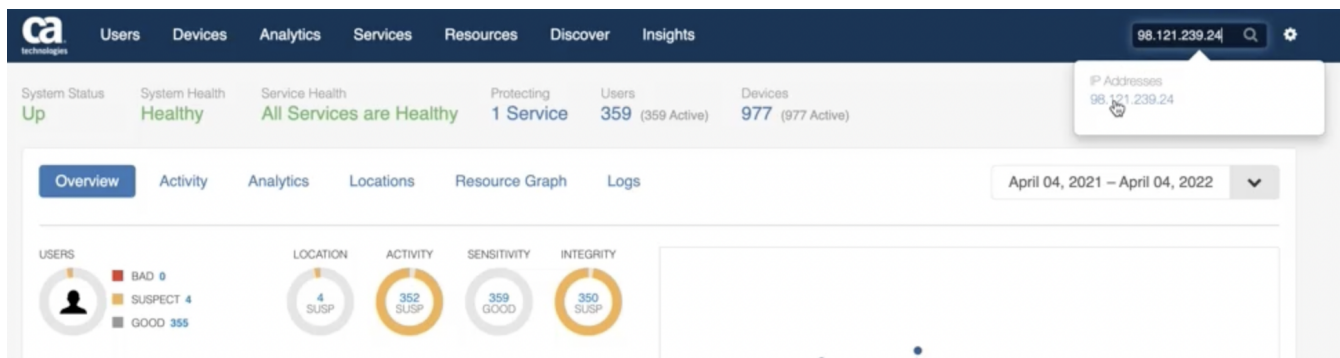
The **Mixing Function** section of the **Advanced** menu allows you to save a copy of the current mixing file to your system. The default location is the Documents folder of the user.



The file that is saved in this example is named `mixing_function.aa4337cc4e08c36c81fed5b1e16ab4e7.mxg`, and its content is not readable to most users. But the file does allow you to save and restore different mixing schemes using the **Update Mixing Function** button.

## Access User Activity Using IP Search

The search field at the upper right corner of the screen can be used to search on IP addresses. Enter the IP address, press the enter key, and then select the blue link that drops down.



You see a list of activity from this IP address that includes the following elements:

- A location map
- The user name
- The devices used
- The start and ending date and times of all IP sessions

At the top of the **IP Sessions** page are fields that monitor the following characteristics:



- The IP address
- The connection type
- The location
- The date of the first appearance on the network for the period specified
- The state of the user
- Counts of the number of sessions, users, and devices in the session

You can specify the start and end dates for the list in the search field at the top-right of the page.

The screenshot shows the Symantec Privileged Access Manager interface. At the top, there is a navigation bar with tabs: Users, Devices, Analytics, Services, Resources, Discover, and Insights. A search bar is located on the right. Below the navigation bar, a summary row displays the following information: IP Address: 10.76.13.123, Connection Type: N/A, Location: N/A, First Seen: May 4, 2022 8:28 PM, State: Active, Session Count: 41, Users Count: 3, and Devices Count: 3. Below this, there is a tabbed interface with 'IP Sessions' selected. A date range filter is set to 'June 20, 2022 – July 20, 2022'. The main content area displays a table of sessions.

User	Devices	Session start	Session end
super ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jul 18, 2022 7:19 PM	Active
super ⓘ	N/A	Jul 18, 2022 7:18 PM	Jul 19, 2022 7:18 PM
super ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jul 13, 2022 2:18 PM	Jul 15, 2022 8:33 PM
super ⓘ	N/A	Jul 13, 2022 2:17 PM	Jul 15, 2022 6:05 PM
super ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jul 11, 2022 2:54 PM	Jul 12, 2022 8:42 PM
super ⓘ	N/A	Jul 11, 2022 2:52 PM	Jul 12, 2022 7:08 PM
super ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jul 5, 2022 2:26 PM	Jul 6, 2022 8:46 PM
super ⓘ	N/A	Jul 5, 2022 2:26 PM	Jul 6, 2022 6:17 PM
Bob Lee ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jun 30, 2022 4:43 PM	Jul 1, 2022 6:14 PM
Bob Lee ⓘ	N/A	Jun 30, 2022 4:42 PM	Jul 1, 2022 6:12 PM
Sam Grant ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jun 30, 2022 4:24 PM	Jul 1, 2022 4:41 PM
Sam Grant ⓘ	N/A	Jun 30, 2022 4:23 PM	Jul 1, 2022 6:12 PM
super ⓘ	6d9dd9cfb3018209ef7bc85ed91555202090faf7370ff3d6db7d6f3d34adf825 ⓘ	Jun 27, 2022 6:48 PM	Jul 1, 2022 7:15 PM
super ⓘ	N/A	Jun 27, 2022 6:47 PM	Jun 29, 2022 2:20 PM

If you select a user or device from the **IP Sessions** tab, it takes you to the **Risk Level Activity** page for that user or device.

The **Activity** tab from the IP Address page lists every session from the specified period of time. This list provides the following characteristics:

- The timestamp of the session
- The user
- The device
- The action that is taken and the resource that is used
- The IP address
- The client

This pane is similar to the **Activity** tab on the **Home** menu, but without the bar graphs.

IP Sessions					
Activity					
Users					
Devices					
Whois					
June 14, 2022 – July 14, 2022					
Timestamp (UTC) ↕	User ↕	Device ↕	Action - Resource	IP/Location	Client
07/14/2022 18:05:30 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/14/2022 18:05:11 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
07/14/2022 18:05:02 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN_FAILURE - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
07/14/2022 18:04:56 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN_FAILURE - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
07/14/2022 16:28:48 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	LOGOUT - CA PAM ⓘ	10.76.13.123 ⓘ	Chrome 90.0.4430.93
07/14/2022 16:28:40 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO_LOGOUT - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/14/2022 15:45:48 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/14/2022 15:42:22 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13
07/13/2022 20:26:53 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	LOGOUT - CA PAM ⓘ	10.76.13.123 ⓘ	Chrome 90.0.4430.93
07/13/2022 20:26:49 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO_LOGOUT - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/13/2022 18:12:13 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/13/2022 18:11:51 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13

Select the **Service Session** link in the Timestamp column to see the details of the individual session on the **Activities** tab.

Activities					
Resource Sessions					
Timestamp (UTC) ↕	User ↕	Device ↕	Action - Resource	IP/Location	Client
07/14/2022 18:05:30 Service Session ⓘ	super ⓘ	6d9dd9cfb3018209ef7bc85ed9155... ⓘ	SSO - tap.ca.com ⓘ	10.76.13.123 ⓘ	Java
07/14/2022 18:05:11 Service Session ⓘ	super ⓘ	Other (Other) running Other 1.8.0_3... ⓘ	LOGIN - CA PAM ⓘ	10.76.13.123 ⓘ	Other Library 4.5.13

Select the **Resource Sessions** tab to see information about the PAM resources used in that session.

Activities						
Resource Sessions						
Service	User	Resource	Resource Session	Session Start	Session End	Session Duration
CA PAM	super ⓘ	tap.ca.com ⓘ	Session Details ⓘ	Jul 14, 2022 6:05 PM	Active	1858 Sec

Select the **Users** tab on the IP search page to see a list of users with their latest risk level decisions, latest location, and the normal/suspect/bad status of all four categories of analytics. This view is similar to the table on the **Users** tab at the top of the screen.

IP Sessions	Activity	<b>Users</b>	Devices	Whois
-------------	----------	--------------	---------	-------

Title ↕ ↑	Latest Risk Level Decision ↕	Latest Location	Location	Integrity	Activity	Sensitivity
scroswell ⓘ Dormant	 Aug 26, 2020 11:42 AM <a href="#">Inspect Incident</a> Never Active In Organizational Operating ...	Atlanta, Georgia, US Active for a day starting Oct 12, 2021				
super ⓘ	 Sep 28, 2021 9:05 PM <a href="#">Inspect Incident</a> Expired - Concurrent Service Sessions	Atlanta, Georgia, US Active for 2 days starting Apr 1, 2022				

Select the **Devices** tab on the IP search page to see session information that is also available on the main **Devices** menu. This view is similar to the **Users** tab but also includes a column for operating systems or the devices.

IP Sessions	Activity	Users	<b>Devices</b>	Whois
-------------	----------	-------	----------------	-------

Title ↕ ↑	OS ↕	Latest Risk Level Decision ↕	Latest Location	Location	Integrity	Activity	Sensitivity
239e1ab7a0c1488e64... ⓘ Dormant	Windows x64/6.3	 Jul 1, 2022 5:31 PM Expired - Bad Associated Risk Sub... Associated with a bad User	Active for a day starting May 4, 2022				
26868d1635154b104a... ⓘ	Windows x86/10.0	 Jun 23, 2022 8:41 PM New Risk Subject New Device	Active for a day starting Jun 23, 2022				
6d9dd9cfb3018209ef7... ⓘ	Windows x86/10.0	 Jun 15, 2022 6:41 PM New Device User New Device User detected	Active for a day starting Jul 13, 2022				

The **Whois** menu provides details about the IP address that is provided by the Whois service from ARIN, a public resource that can retrieve essential information about the address, including the following information:

- The network range, network name and handle, network type and its parent
- The organization that owns the site and the registration dates of the IP address
- The name and address of the owner
- Other useful information

IP Sessions Activity Users Devices **Whois**

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#
```

```
NetRange: 98.120.0.0 - 98.123.255.255
CIDR: 98.120.0.0/14
NetName: RRMA
NetHandle: NET-98-120-0-0-1
Parent: NET98 (NET-98-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Charter Communications Inc (CC-3517)
RegDate: 2008-04-09
Updated: 2008-04-09
Ref: https://rdap.arin.net/registry/ip/98.120.0.0
```

```
OrgName: Charter Communications Inc
OrgId: CC-3517
Address: 6175 S. Willow Dr
City: Greenwood Village
StateProv: CO
PostalCode: 80111
Country: US
RegDate: 2018-10-10
Updated: 2021-11-01
Comment: Legacy Time Warner Cable IP Assets
Ref: https://rdap.arin.net/registry/entity/CC-3517
```

98.121.239.240

# Administrating

---

The content in this section describes administrative procedures.

**Use the table of contents to access the topics in this section**

## Account Types

### 'super' (root account)

Privileged Access Manager has two preconfigured user accounts: 'super' and 'config'. The 'super' is a superuser (or root) account that has access to all Privileged Access Manager settings (and thus the config account settings). As with the config account, super cannot be deleted.

1. Point your browser to the Privileged Access Manager URL.
2. When you log in for the first time, accept the license agreement. Select **I Agree** to continue.
3. Enter your default "root" credentials (**User:** super / **Password:** super) and select **ENTER**.
4. The first time that you log in:
  - a. You see at least two requests to accept Java. If your Java console has been set on, you see the Java console startup too.
  - b. You see the **User Information** dialog. Several fields are available for edit, but you are required to change at least the default password ("super").
5. Change the password by using the fields **Old Password**, **New Password**, and **Confirm Password**.  
The strength of the new password must conform to Security Level 2, which requires that the updated password:
  - a. Differ from the previous password
  - b. Have a length between the Global Settings values for **Min Length** (default: 6) and **Max Length** (default: 14)
  - c. Have at least one (Latin) alphabet character
  - d. Have at least one numerical digit character
6. Change any other fields that are desired, and select **OK**.  
A warning message appears: "Configuration Password is still the default value." Address this warning now, as described in **'config' (root account)**.
7. Select **Logout** at the upper right-hand corner.

### 'config' (root account)

We recommend that you use this configuration account only for initial setup. Change the password from default using the Change Password button in the Toolbar Menu. Consider also changing the "config" Login Id in addition to the Password using the Change Password menu. Store the password in a safe place and use it only for emergencies when other authentication methods are not available.

This account is used only for Privileged Access Manager configuration. For information about resetting its name or password, see [Change Login for Config or Super User](#).

### Provisioned Users

All other Users that you create, regardless of their roles, are initially presented with the My Info page for password change. After they change their passwords, they land on the default page suitable to their roles.

- Global Administrators (including the 'super' account), Operational Administrators or Server Control Administrator roles land on the Dashboard Overview Tab.
- Most End Users (with the "Standard User" role) land on the **Access** page (whether it is populated with any access links). They do not see the rest of the dark gray menu bar.
- Other Users with various combinations of roles land on the **Access** page, but also see a customized administration menu bar.
- The 'config' account has access only to the **Configuration** menu, and cannot access the rest of the administration menu.

## Dashboards

Learn about the PAM Overview, System, and Cluster Dashboards.

PAM provides the following dashboards to monitor different aspects of your environment:

- The [Overview Dashboard](#) provides a centralized view of your PAM Environment.
- The [System Dashboard](#) shows current and historical system data about a single PAM node that allows you to visualize system performance and identify trends over time.
- The [Management Console Cluster Dashboard](#) shows current and historical system data about a cluster that allows you to visualize cluster performance and identify trends over time.

## Overview Dashboard

Learn how to use the Overview Dashboard (formerly known simply as the Dashboard) to monitor functional information about your PAM environment.

### Introduction

PAM provides Overview and System dashboards to monitor the functional information about your environment.

The Overview dashboard provides a centralized view of your PAM Environment. This dashboard shows a summary of key managed elements and counts newly added items, breakdown of logins and sessions currently in progress, list of violation log events, appliance and cluster health.

The Overview dashboard provides a centralized view of your PAM Environment, including:

- Access requests: View counts of approved access requests.
- Security alerts: View and respond to security alerts, such as suspicious login attempts and unauthorized access.
- System health: Monitor the performance and health of your PAM environment.
- At-a-glance view of privileged access activity: The dashboard provides a summary of all privileged access activity, including the number of active sessions and applications used.
- Threat Analytics Console that identifies anomalies in PAM user behavior and implementing policies to dynamically mitigate potential insider threats or breaches by external threat actors.

### **NOTE**

The Overview Dashboard is only present in the PAM UI if you are logged in with an account with Global Administrator, Operational Administrator, or Server Control Administrator roles.

To access the Overview Dashboard, select **Dashboard** in the menu bar and then select the **Overview** tab that appears below the menu bar, as shown in the following screen capture:



Symantec PAM Manager

Dashboard Sessions ▾ Users ▾

Overview System Metrics

## Dashboard

### Overview Dashboard Panel Components

#### **Messages**

Privileged Access Manager puts information for the user under the Dashboard heading.

#### **Elements Under Management**

This panel displays the current quantities of various managed elements, highlighting recent additions. Selecting an icon navigates to the respective view of the elements.

- **Devices** – Target Devices in use (all types)
- **Device Groups** – Device Groups in use
- **SC Policies** – Server Control Policies in use
- **SC Devices** – Server Control Devices in use
- **Privileged Accounts** – Privileged user target accounts registered and recently added account total
- **A2A Accounts** - A2A target accounts registered and recently added account total.
- **Users** – User accounts registered
- **A2A** – Accounts
- **Target Applications** – Target applications registered and recently added application total.
- **Vaults** – Vaults in use
- **Secrets** – Secrets in use
- **Credential and Vault Management** – For password and vault management target account use

#### **Session Management**

- **Logins** shows the number of currently active User login sessions. This number includes multiple logins of the same User (when applicable).
- **Sessions** shows the number of currently active connection sessions. This number includes multiple connections from the same User to the same Device (when applicable).

#### **Credential Management**

Credential Management shows the top four counts from Credential Manager Activities Reports. These reports are configured at **Credentials, Reports, Activities**. Any four of these report values might be reported here:

- Passwords used in last 30 days
- Password requests pending
- Passwords not verified
- Clients requiring activation
- Proxies requiring activation
- Passwords changed today
- Failed A2A client requests in last 30 days
- Successful A2A client requests in last 30 days
- All A2A client requests in last 30 days
- Unverified compound accounts
- Synchronized accounts with expired passwords
- Unsynchronized accounts with expired passwords

### ***Appliance Status (or Cluster Status)***

Per Hardware Appliance. The order of the appliances is the same as that in **Configuration, Clustering**.

- **CPU:** CPU capacity in use during the selected time period
- **RAM:** Memory in use during the selected time period
- **HDD:** Disk storage in use during the selected time period
- **Network Share:** Network share in use; only visible if a network share has been added for session recording or database backups
- **Hostname:** Hostname assigned
- **IP:** IP Address that is assigned
- **MAC:** Address assigned
- **Machine Type:** for example, Standard
- **Status indicator :** Displays current status

### ***License Usage***

**Quantities currently:** (In Use) / (Licensed)

- **Session Management** – For device access use
- **Credential Management** – For password management target use
- **A2A Management** – For A2A request server use
- **Server Control Management** – For Server Control device use

### ***Recent Events***

Time and Details of messages for recent connection and violation log events. The most recent events are listed first.

### ***Server Control Administrator Dashboard***

When a user with the Server Control Administrator role logs in, the Dashboard displays the following components:

- **Elements Under Management:** Devices, Device Groups, SC Policies, SC Devices, Users
- **Appliance Status:** CPU, RAM, HDD, Hostname, IP, MAC, Machine type, Status Indicator
- **License Usage:** Server Control Management
- **Recent Events**

### ***Analytics***

When the Threat Analytics component is enabled, the Analytics panel appears in the center/bottom of the Dashboard. Selecting the icon launches the **Threat Analytics** console that identifies anomalies in PAM user behavior. Selecting the **Threat Analytics** icon also implements policies to dynamically mitigate potential insider threats or breaches by external threat actors.



## Analytics

### Threat Analytics



To enable the Threat Analytics component, see [Implementing Threat Analytics](#) for more information.

## System Dashboard (Single Node)

Learn how to use the System Dashboard data visualization tool to view and interpret information about a single PAM node.

### Introduction

The System Dashboard is a visualization tool that shows current and historical system data that dynamically updates with time, allowing you to monitor system performance and identify trends. The System Dashboard shows system data about a single PAM instance.

The following screenshot shows some sample System Dashboard output:

## PAM Details ⓘ

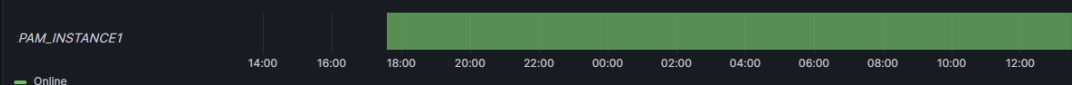
```
Cluster:
Site:
PAM:PAM_INSTANCE1
CPU: 8
RAM: 8 GB
Disk: 9.70 GB
```

## Access Activity History ⓘ

Mode

## Online

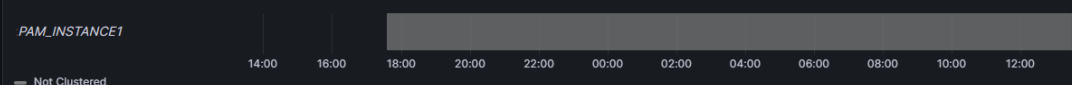
Mode History



Sync Status ⓘ

Not Clustered

Sync History ⓘ



## RAM Current ⓘ



## RAM History ⓘ



## CPU Current ⓘ



## CPU History ⓘ

## Disk Utilizati... ⓘ



### PAM OS Disk Utilization History

### Session Recording Storage History ⓘ

### Backup Session Recording Storage History ⓘ

No data

### Disk IO History

### Network IO History

## Access the System Dashboard

You can access the System Dashboard for a PAM instance from the PAM Client or a supported web browser.

### NOTE

Microsoft Edge running in Internet Explorer mode does not support the System Dashboard.


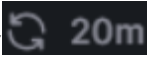
To access the System Dashboard, use one of the following options:

- Log in to a PAM instance using an account with either the Global Administrator or Operational Administrator role. The Overview Dashboard opens. Select **Dashboard, System** to open the System Dashboard.  
To return to the System Dashboard after navigating elsewhere in the UI, select **Dashboard** in the menu bar. If you have used the Overview Dashboard, select the **System** tab to open the System Dashboard.
- Log in to the Management Console using an account with either the Global Administrator or Operational Administrator role. The console lists all the clusters in your environment. To open the System Dashboard with the Management Console instance information, follow these steps:
  - Select **Administration**. The Overview Dashboard opens.
  - Select **Dashboard, System**.

## Refresh the Dashboard Data

By default, the dashboard does not update automatically to preserve system resources.



To update the data manually, select the **Refresh** icon () near the right end of the menu bar.

To configure the dashboard to refresh the data automatically, select the **Auto/Manual Refresh** icon () at the far right of the menu bar, and then choose **Auto** from the drop-down menu. The refresh time adjusts based on the time duration that is selected in the time option. The **Refresh** icon is updated to reflect the change (.

## Modify the Displayed Time Range

By default, the dashboard visualizations show data from the last 24 hours. PAM purges data older than 30 days.

Use either of the following methods to modify the range of time displayed:

- Click and drag over an activity timeline to zoom in.
- Select the **Time Range** button () in the menu bar and choose from a list of preset ranges or specify an absolute range on the **Time Range** dialog that opens.
- If a time range is displayed in the menu bar beside the **Time Range Zoom** button, use the lesser than (<) and greater than (>) buttons to shift the timeline forward and backward. The duration between the selected times remains constant.
- Select the **Time Range Zoom** button () in the menu bar to zoom out.

The selected time range is applied to the activity timelines and all other data on the dashboard shifts to reflect the same time period.

### IMPORTANT

Current status elements (for example, meters) also shift with the timeline but display the data applicable at the end of the selected time range (if that is not the current time).

## System Dashboard Components

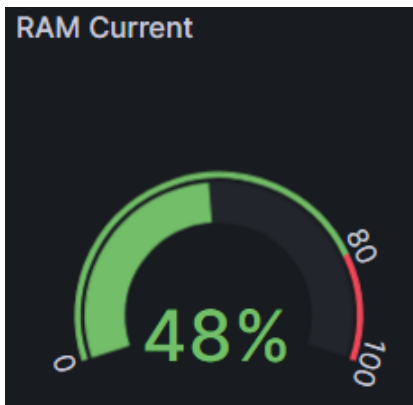
This section describes all the data that the system dashboard provides about the current PAM instance, separated into functional groups.

### System Dashboard Visualization Elements

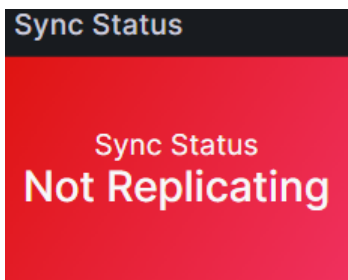
The dashboard presents system data using one or both of the following visualization elements:

- **Current status:** A meter or text box that describes current status as shown in the following example screenshots:

Example status meter:



Example status text box:



- **Activity Timeline:** A chart that shows status over time, as shown in the following example screenshot:



## System Health

The dashboard provides the following usage metrics for standard indicators of server system health.

### NOTE

**RAM, CPU, and Disk** charts select the line color to reflect the most-recent value. For example: if a line peaks above the threshold but the last data point (based on the given timeline) is below the threshold, the entire line appears green.

- **RAM:** Memory in use during the selected time period
- **CPU:** CPU capacity in use during the selected time period
- **Disk:** Current status within the activity timeline
- **Session Recording Storage** (primary NFS/CIFS mount) status: Activity timeline only.
- **Backup Session Recording Storage** (secondary NFS/CIFS mount) status: Activity timeline only.
- **Disk IO** status: Activity timeline only.
- **Network IO** status: Activity timeline only.

## Operational Health

The dashboard provides the following usage metrics about indicators of PAM operational health:

- **Mode** (Online or Maintenance): Current status and activity timeline.
- **Sync Status** (Online, Not Clustered, or Not Replicating): Current status and activity timeline. Not Clustered appears for PAM instances that are not part of a cluster.

## Access Activity

The dashboard provides the following usage metrics about PAM access activity:

- **PAM Logins** (users logged in): Activity timeline only.
- **PAM Sessions** (active access sessions): Activity timeline only.

## Interpret the Dashboard Data

Resource utilization on PAM appliances can exhibit short bursts or drops in activity levels, affecting both OS metrics like RAM and CPU usage, as well as physical resources like disk and network I/O.

In virtualized environments such as VMWare, KVM, and cloud platforms, the underlying physical infrastructure is shared among multiple VMs. PAM reflects the availability and allocation of resources to individual VMs, essentially scheduling and allocating resource capacity slots for their operation.

Under conditions of infrastructure strain, heavy load, or operations like snapshots, the overall performance of VMs may be impacted. While the effect is typically minimal, there may be instances where VM processing is completely paused or allotted resources are reclaimed to accommodate higher-priority activities.

**To avoid unnecessary concerns when evaluating PAM dashboard activity timelines, consider the following important factors:**

- **Magnitude of changes:** Assess the extent of resource utilization fluctuations. Consider orders of magnitude differences.
- **Episode duration:** Determine the duration of these fluctuations, distinguishing between quick blips and sustained periods of abnormal resource usage.

## What to look for in the dashboard:

- **Activity timeline chart time range:**
  - Examine the charts. Even if a chart appears to have a significant spike, if the time range is low or has a very narrow range, the visualized spike may not be a cause for concern.
  - However, if the scale is large and the meter remains high over an extended period, it is worth investigating. Keep in mind that while PAM may be busy, overall performance and response times may still function normally without degradation.
- **Interpret short spikes:**
  - Brief spikes are normal day-to-day behavior for VMs, appliances, and operating systems. Therefore, an infrequent spike in a chart does not necessarily indicate a problem.
  - However, long durations of elevated activity should warrant further investigation.
- **Identify performance issues:**

- When PAM performance issues occur, use the dashboard to identify when health and performance issues began and time windows when intermittent issues reoccur.
- Use the dashboard to highlight unexpected changes or changes that occur slowly over time.

## Management Console Cluster Dashboard

Learn how to use the Management Console Cluster Dashboard data visualization tool to view and interpret information about your cluster.

### Introduction

The Cluster Dashboard is a visualization tool that shows current and historical system data about a PAM cluster that dynamically updates at specified intervals. The Cluster Dashboard is a valuable tool for monitoring cluster performance and identifying trends over time. The following screenshot shows some sample Cluster Dashboard output:

Cluster Name PAM\_CLUSTER1 PAM Site Name All PAM Instance Name All

### Cluster Details

## Cluster Information ⓘ

Cluster Name: *PAM\_CLUSTER1*  
PAM Site: *site1, site2*

### PAM Licenses Utilization



## Access Activity ⓘ

### Cluster Node Details

## PAM Health Details ⓘ

Cluster Name	Site	Node	Logins	Sessions	Maintenance	Synchronization	Network I	RAM	CPU	PAM OS Disl	Rec. Primary Disk
PAM_CLUSTER1	site1	PAM_NODE1	4	0	Online	Up To Date	0.04%	74.6%	2%	20.6%	75.0%
PAM_CLUSTER1	site1	PAM_NODE2	0	0	Online	Up To Date	0.03%	69.2%	3%	16.4%	75.0%
PAM_CLUSTER1	site2	PAM_NODE3	0	0	Online	Up To Date	0.01%	81.7%	1%	20.1%	

### Sync Status Over Time

#### Sync Status History



## PAM Statistics ⓘ

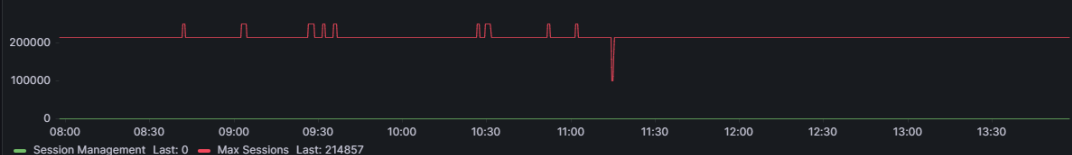
Devices	Device Groups	SC Policies	Target Applications	Users	Privileged Accounts	A2A Devices	SC Devices	Secret Vaults	Secrets
0	18	13	7	5	2	0	0	0	0

### ~ Licenses Over Time

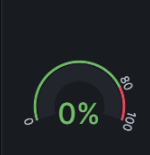
Sessions ⓘ



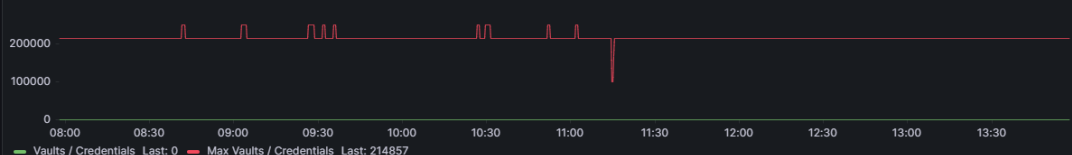
Session License History ⓘ



## Vaults / Credentials



Vault / Credential License History ⓘ



## A2A ⓘ



## A2A License History ⓘ

## Server Control ⓘ



Server Control License History ⓘ

## Access the Cluster Dashboard

To access the **Cluster Dashboard**, do the following steps:

1. Log in to the Management Console from the PAM client or a supported web browser using an account with either the Global Administrator or Management Console Administrator role.


### NOTE


Microsoft Edge running in Internet Explorer mode does not support the System Dashboard.


2. Select the cluster whose data that you want to visualize from the list of clusters that appear.
3. Either select the **View Dashboard** button, or choose **View Dashboard** from the **Actions** column.

## Refresh the Dashboard Data

By default, the dashboard does not update automatically to preserve system resources.

To update the data manually, select the **Refresh** icon () near the right end of the menu bar.



To configure the dashboard to refresh automatically, select the **Auto/Manual Refresh** icon () at the far right of the menu bar, and then choose **Auto** from the drop-down menu. The refresh time adjusts based on the time duration that is

selected in the time option. The **Refresh** icon is updated to reflect the change ()

## Modify the Displayed Time Range

By default, the dashboard visualizations show data from the past 24 hours. PAM purges data older than 30 days.

Use either of the following methods to modify the range of time displayed:

- Click and drag over an activity timeline to zoom in.
- Select the **Time Range** button () in the menu bar and choose from a list of preset ranges or specify an absolute range on the **Time Range** dialog that opens.
- If a time range is displayed in the menu bar beside the **Time Range Zoom** button, use the lesser than (<) and greater than (>) buttons to shift the timeline forward and backward. The duration between the selected times remains constant.
- Select the **Time Range Zoom** button () in the menu bar to zoom out.

The selected time range is applied to the activity timelines and all other data on the dashboard shifts to reflect the same time period.

### IMPORTANT

Current status elements (for example, meters) also shift with the timeline but display the data applicable at the end of the selected time range (if that is not the current time).

## Cluster Dashboard Components

The **Cluster Dashboard** provides the following data about the selected PAM cluster:

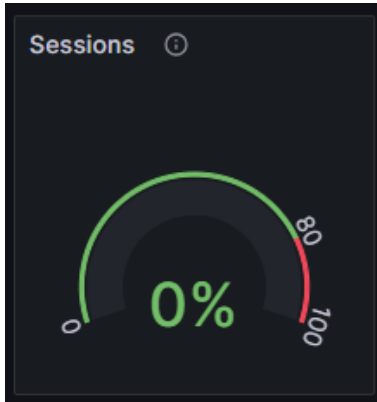
### Cluster Dashboard Visualization Elements

The dashboard presents system data using one or both of the following visualization elements:

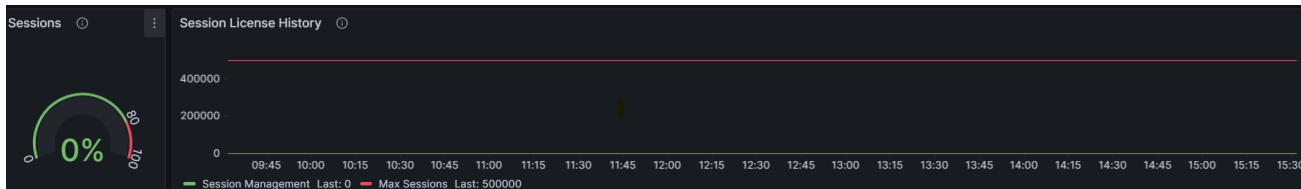
- **Current status:** A meter or text box that describes current status as shown in the following example screenshots:

Example status meter :





- **Activity Timeline:** A chart that shows status over time, as shown in the following example screenshot:



- **Access Activity:** Aggregated usage metrics about PAM access activity across the cluster:
  - **PAM Logins:** The number of currently active user login sessions. This value includes multiple logins of the same user (when applicable).
  - **PAM Sessions:** The number of currently active connection sessions. This value includes multiple connections from the same User to the same Device(when applicable).
- **PAM Licenses Utilization:** Overall license usage at the latest data point within the selected time range:
  - **Session Management**
  - **Vaults / Credentials:** Vaults in use
  - **A2A:** The accounts in use
  - **Server Control:** Server Control license use
- **Cluster Node Details:** Health and access information for each node in the cluster:

- **Cluster Name:** the name of the cluster
- **Site:** the name of the site
- **Node:** The name of the node. Select the name to view the System Dashboard for the individual node.
- **Rec. Primary Disk:** Session Recording disk in use
- **Logins:** The number of currently active user login sessions.
- **Sessions:** The number of currently active connection sessions.
- **Maintenance:** Online or Maintenance.
- **Synchronization:** This detail reflects the replication status.
- **Network IO:** The network input/output
- **RAM:** Memory in use during the selected time period.
- **CPU:** CPU capacity in use during the selected time period.
- **PAM OS Disk:** OS in use
- **Sync Status Over Time:** Activity timelines showing the synchronization status for each node.
- **PAM Statistics:** A bar of status boxes that show the current usage of a number of managed

PAM Statistics ⓘ									
Devices	Device Groups	SC Policies	Target Applications	Users	Privileged Accounts	A2A Devices	SC Devices	Secret Vaults	Secrets
0	18	13	7	5	2	0	0	0	0

elements:

- **Licenses Over Time:** Meters showing license usage at the latest data point within the selected time range and Activity timelines showing usage over time:
  - **Sessions:** The number of currently active connection sessions.
  - **Vaults / Credentials:** The password and vault management target accounts in use
  - **A2A:** Accounts
  - **Server Control:** Server Control device licenses use

### Interpret the Dashboard Data

Resource utilization on PAM appliances can exhibit short bursts or drops in activity levels, affecting both OS metrics like RAM and CPU usage, as well as physical resources like disk and network I/O.

In virtualized environments such as VMware, KVM, and cloud platforms, the underlying physical infrastructure is shared among multiple VMs. PAM reflects the availability and allocation of resources to individual VMs, essentially scheduling and allocating resource capacity slots for their operation.

Under conditions of infrastructure strain, heavy load, or operations like snapshots, the overall performance of VMs may be impacted. While the effect is typically minimal, there may be instances where VM processing is completely paused or allotted resources are reclaimed to accommodate higher-priority activities.

**To avoid unnecessary concerns when evaluating PAM dashboard activity timelines, consider the following important factors:**

- **Magnitude of changes:** Assess the extent of resource utilization fluctuations. Consider orders of magnitude differences.
- **Episode duration:** Determine the duration of these fluctuations, distinguishing between quick blips and sustained periods of abnormal resource usage.

### **What to look for in the dashboard:**

- Activity timeline chart time range:

- Examine the charts. Even if a chart appears to have a significant spike, if the time range is low or has a narrow range, the visualized spike may not be a cause for concern.
- However, if the scale is large and the meter remains high over an extended period, it is worth investigating. Keep in mind that while PAM may be busy, overall performance and response times may still function normally without degradation.
- Interpret Short spikes:
  - Brief spikes are normal day-to-day behavior for VMs, appliances, and operating systems. Therefore, an infrequent spike in a chart does not necessarily indicate a problem.
  - However, long durations of elevated activity should warrant further investigation.
- Identify performance issues:
  - When PAM performance issues occur, use the dashboard to identify when health and performance issues began and time windows when intermittent issues reoccur.
  - Use the dashboard to highlight unexpected changes or changes that occur slowly over time.

## Session Management

The **Sessions** option on the menu bar allows several production-stage administrative activities:

- **Manage Sessions** – View and control (authenticate/terminate/record) user login and connection sessions.
- **Logs** – View the session log entries, which show user session activity.
- **Session Recordings** – View a list of recordings, and optionally view any recording (in a separate viewer application).

### View the List of Managed Sessions

The **Manage Sessions** page shows a list of the current user sessions. The columns in the table include:

- **User:** Shows the login session for a specific user.
- **Duration:** Indicates a single instance of a connection to a device within a login session. A single line-item within a User login item represents a session. Each user login can independently establish a session with a device. As with similar lists throughout the Administration menus, the list can be ordered on any user login column.
- **Timeout:** Indicates the time remaining until the login session times out. After the session expires, the user is automatically logged out.
- **Type** - Describes the session type, such as Access.
- **Authentication Type** - Indicates whether authentication is local or remote.
- **Connections** - Shows the number of connections that are made by a user.

Idle time is the duration in which there is no communication between the client UI and Privileged Access Manager.

Do not confuse the Timeout setting for the user session with the Login Timeout global setting. If Login Timeout is set to zero at the time the user session is established, the Timeout value for the session is always "NEVER".

When the corresponding Login Session begins an active Connection Session, the Timeout countdown is suspended. In place of the current Timeout value, there is a **UNDVC** placeholder. When every active session closes, the Timeout countdown resets to the global Login Timeout value, and a new countdown begins. When the Timeout value is changed while a Login Session is active, that Login Session continues to use the previous Timeout value.

### Manage Individual User Sessions

From the **Manage Sessions** page, you can select a currently logged-in user from the list and take the following actions:

- **View**— Select View to display information about the user, such as name, email,
- **Logout** – Select Logout to terminate the session for the user.
- **Re-authenticate** - Select Reauthenticate to force the user to log in again. Forcing users to reauthenticate suspends any active applets. This setting also stops the ability to perform administrative function until you give your password. After you provide your password, your session resumes where you left off.

### **Manage Sessions Using Selected Criteria**

The **I WOULD LIKE TO** button on the Sessions page lets you control user and device connection sessions for one or more sessions. For instructions about using this control, go to [Manage Sessions Based on Specific Criteria](#).

## **View Session Logs and Reports**

Use the session log to monitor user behavior and to prevent suspicious activity. You can then view log data in reports that are included with the product or in reports you create.

### **Unfiltered Log Records**

When you select **Sessions, Logs**, you see an unfiltered listing of all recent activity. The unfiltered log entries show a subset of all fields and wrapped-line field data. To display the full set of field data for a log entry, select once on a log entry to open it. To modify the display of the unfiltered log, select in the heading, then the resulting triangle to select **Columns**. Select the boxes that you want to display.

When you exit the Logs page, the column settings are saved.

### **Filter Logs to Focus Entries**

View a more focused list by filtering the display of entries.

#### **Follow these steps:**

1. Verify that you are looking at the unfiltered list.
2. At the top of the list, select a column type then enter a relevant value in the **Value** field.  
For some column types, a new window opens, from which you can select an available value.
3. Optionally, add more criteria by selecting **Add Filter**.
4. Select **Filter**.  
The list is updated with only the records matching the filter selections.

### **View Predefined Reports**

You can view logs in various report formats. These formats include:

- Payment Card Industry (PCI) Data Security Standard (DSS) reports included with the product.
- Reports that you create.

#### **Follow these steps to see a specific report:**

1. Select **Sessions, Logs**.
2. Under the **Reports** drop-down list, a list of existing reports (and, for custom reports, their owner) displays.  
Pre-configured PCI reports are in the list.
3. Select a pre-defined report to view.

To see the unfiltered list again, select **Unfiltered Logs**.

### **Create, Update, and View Custom Reports**

Use this procedure to create, update, or view custom reports that contain your choice of log data.

**NOTE**

Any user with privileges to view logs can create a custom report. Custom report names are appended with the user ID of their author for easy identification.

**Follow these steps:**

1. Select **Sessions, Logs**.
2. From the **Reports** drop-down list, select one of the following options:
  - To create a new custom report, select **Save As**.
  - To modify a report that you created, select that report from the list and select **Save**.
  - To view, update and manage existing reports, select **Manage Reports**. A dialog opens displaying a list of reports that you can view, update, or delete depending on their type (custom or preconfigured), your privileges, and ownership.

**NOTE**

Only the user that created a custom report (its owner) or the Global Administrator can update or delete that report. To quickly locate reports that were created by a particular user, filter the report list by "Owner User Id".

Preconfigured reports show no owner and can only be viewed.

3. If you chose to create or update a report, use the following tabs on the dialog that appears to design the report:
  - **Basic Info:** Enter a Name (required) for the report. Enter other fields as appropriate. Most of the tabs are self-explanatory.
  - **Date Range:** Enter specific dates or select **Relative**. The Relative range produces a report for your specified number of days, weeks, or months *before* the time of the report.
  - **Transactions:** Select from the list of available transactions the activities you want in the report.
  - **Users/Groups:** Select from the list of available users and groups those people whose activity you want in the report.
  - **Devices/Groups:** Select from the list of configured devices and device groups those systems that you want to in the report.
  - **Applets:** Select from the list of available service applets the ones you want in the report.
  - **Columns:** **Select all the columns that contain the type of information you want in the report.**
  - **Email:** To replicate the report at a regular interval and send it by email to specific individuals, select **Send Emails**. More fields display.
    - a. Enter email addresses in **Emails**, comma-delimited
    - b. Specify the intervals to send emails.
4. Select **OK** to save the report.

**Download a Report**

You can download any report as a comma-separated value (CSV) file. Use the report in spreadsheets or other applications.

**View Session Recordings**

This content describes how to view recorded sessions in the Session Recording Viewer.

**Open a Recording in the Session Recording Viewer**

Use this procedure to open a recording in the Session Recording Viewer.

**NOTE**

If you attempt to open a recording and receive a PAM-UI-2106 error message, the recording may be on a different share to which another PAM appliance is pointing. To view this recording, login to the PAM appliance that handled the access session and view the recording there.

**Follow these steps:**

1. Select **Sessions, Session Recording**
2. Select **View Recording** in the right-hand column of the file of interest.  
The Session Recording Viewer opens loaded with the selected recording.

**Session Recording Viewer Fields and Controls**

Within the Session Recording Viewer, you see the following information:

- **Session info** In the top segment of the upper-left panel, information about the session and its recording is displayed:
  - **Server:** target hostname or IP Address
  - **Security Layer:** NLA (TLS 1.2) | TLS (1.1) | TLS (1.0) | TLS (TLS 1.0) | TLS (1. 1) | TLS (1.2) | RDP
  - **Encryption Level:** High | Client Compatible | Low | FIPS Compliant | Not Applicable  
If Security Layer is SSL, then Encryption Level is shown as Not Applicable, regardless of FIPS status.
  - **Source IP** client hostname or IP Address
  - **Resolution:** pixels x pixels (graphical recordings only)
  - **Quality:** High | Medium | Low (web session recordings only). This setting is for web recording bit depth. Locate the setting from Settings, Global Settings, Applet Customization, Web Recording Bit Depth.
  - **Duration:** HH:MM:SS Start time, using the PAM server time zone. This setting is not used for CLI recordings. For the recording date, see the timestamp of recording.
  - **Start:** Start time, including Time Zone (not used for CLI recordings).
  - **End:** End time, including Time Zone (not used for CLI recordings).
- **User info** In the middle segment of the upper-left panel, information about the Privileged Access Manager and target users is displayed:
  - **User:** target user login ID (*when applicable*).
  - **Domain:** target user domain (*when applicable*)
  - **PAM ID:** appliance name (if available) or address.
  - **PAM User ID:** login ID
- **Recording info** In the bottom segment of the upper-left panel, information about the recording itself is displayed:
  - **Recording type:** ssh | RDP | TELNET | TN3270 | TN5250 | VNC | Web
  - **Size:** Filesize (KB)
  - **SHA verification** status for recording file: In progress... | Valid | FAILED
- **Events** In the lower-left panel, any violations that occurred are listed under **Events**:
  - **Type:** Violation or Text (icons)
  - **Time of Event:** HH:MM:SS
  - **Description:** Brief generic description of violation or text activity

Use the following controls to move through the session:

- Use the play buttons at the bottom center-right portion of the panel. (Play buttons are not available on CLI recordings.)

- **Step Backward** – Causes a 5 second jump backward
- **Play/Pause**
- **Stop** – upon re-Play, returns to beginning
- **Fast Forward** – Switch to run at 2x, 4x, or 6x actual speed (normal)
- **Step Forward** – causes a 5-second jump forward
- Drag the progress cursor across the timeline.
- Near the lower-left corner, enter figures in the **Jump to time** field to skip to any point in the session. The time of the position in the recording shows in the lower right corner, with the duration and the current progress.

### **Resize the Viewer Output for GUI Recordings**

When Initially opened in the Session Recording Viewer window, the recorded GUI fits against the inside border of the presentation area. Use the following options to resize the output:

- Activate the dynamic resizer option by selecting **Operation, Auto Scale** (or by typing Ctrl-A).
  - While *selected*, the GUI expands or contracts against the inner frame of the window as you resize the viewer. Meanwhile, it displays the new linear dimension (width or height) as a percentage of the original GUI length. After you stop resizing the viewer, this linear dimension box fades away.
  - When *unselected*, the viewer freezes the GUI to the size of the current inner frame. The frame no longer changes size as you expand or contract the viewer.
- A reset option, **Operation, Original Size (1:1)** (Ctrl-R), to resize the recorded GUI to its original dimensions immediately
- Keyboard shortcuts
  - Use **Ctrl +** to zoom in and expand the recorded window in 5 percent increments
  - Use **Ctrl -** to zoom out and contract the recorded window in 5 percent decrements
- Keyboard-mouse shortcuts
  - Press **Ctrl** while moving the mouse (scroll) wheel up to zoom in and expand the recorded window
  - Press **Ctrl** while moving the mouse (scroll) wheel down to zoom out and contract the recorded window
- Mouse panning:
  - If the recorded window is larger than the viewing window (not completely in view), you can pan with the mouse. Hold the mouse wheel down to grab and move the recorded window, so that the viewing window pans across the recorded window.
- Zoom control: When you select the magnifying glass icon to the left of the navigation buttons, a zoom control slider is available. This widget provides you fine-tuned control of the size of the recorded GUI:
  - When you move the slider button up or down, you can resize the recorded window in a continuous motion.
  - By selecting the plus or minus of the zoom control, you can increase or decrease the recorded window in 1 percent increments.
  - The *maximum* size of the recorded window is 200 percent of its original linear size. The *minimum* size is 180 pixels on the shorter of the two dimensions (height or width).  
For example: You can zoom in (expand) a 640 x 480 pixel window so that you view 1280 x 960 pixels. Zoom out (reduce) the window to see an actual viewing size of 240 x 180 pixels.

### **Search Text Within a CLI Recording**

Within a CLI Access Method applet recording, you can perform text string searches.

#### **Follow these steps:**

1. From the recording viewer menu bar, select **Operation, Find** to open a text-search panel above the display.
2. To the right of **Find what**, enter a string into the text box. Optionally, select checkboxes to restrict the search to **Match case** or to match only a **Whole word**.

3. Select the arrows next to the text box to reposition the window to the next instance of the search term on the top line.
4. Continue selecting the arrow to continue locating matches.

At the end of the recording file, the search returns to the top. You are also notified with a pop-up message.

### **Disrupted Audit Session Recordings**

If a mount is unavailable, session recording terminates. The recording file is deleted during post processing and an error like the following text is written to the session logs:

```
Recording file contains only file header packet. Possibly the remote server is powered
off
or security settings are too high. Deleting the file:
gk72-0000001518-20130322092630268_RDP
```

### **View Policy Violations in Session Recordings**

Use *one* of the following methods to two ways to view a recorded applet or web portal session:

- **Use the Session Recording list**  
Select **View Recording** at the right of the **red violation line** record in the **Session Recording** list. The Session Recording Viewer window launches, and starts playing from the beginning of the session.
- **Search the logs**  
To search the logs, following these steps:
  - a. Select **Sessions, Logs**.
  - b. In the upper-right hand corner of list, select **Search**.  
The Advanced Search pop-up window appears.
  - c. Set the Transactions to Violations, and select Search (at bottom of pop-up).  
If a policy violation has occurred in an RDP applet session, a **View Recording** button appears in its record.
  - d. Select the **View Recording** button to bring up the RDP Session Recording Viewer. The recording begins a moment before the time of the violation.

## **Manage Sessions By Specific Criteria**

You can control an ongoing individual session or group of sessions according to a set of actions and criteria.

**To manage sessions in progress, follow these steps:**

1. Navigate to **Sessions, Manage Sessions**.
2. Select the **I WOULD LIKE TO** button.
3. Select the action that you want to perform on a session or sessions from the **Action** drop-down list. The following actions are available:
  - Logout
  - Re-Authenticate
  - Disconnect
  - Record
  - Stop

See the table at the end for details about each action.

### **NOTE**

Do not select the Record or Stop action for a session that uses VNC access to a Windows system. You can manage session recordings using these actions only for new sessions that have not yet started.



4. Select the criterion to specify which *type* of session or sessions to control from the **Criteria** drop-down list. The **Criteria** drop-down list is context-sensitive based on the specified action.  
If you select the **Logout** or **Re-Authenticate** actions, the following criteria are available:
  - All
  - User
  - Group
  - Auth. Type
 If you select **Disconnect**, **Record**, or **Stop** actions, the following criteria are available:
  - All
  - Device
  - Group
  - Location
  - Address
  - Port
5. If you did not select **All** in the **Criteria** field, specify which session or sessions to control from the **Value** drop-down list. The Value drop-down list is context-sensitive. For example, if the specified criteria is **User**, a list of current login sessions displays. If the specified criteria is **Disconnect**, a list of current connection sessions to target devices displays.
6. Select **APPLY** to perform the selected action on the applicable users or devices.

### **Applying Actions**

The following table shows what happens when each action is applied.

Action	Behavior
Log out	<ol style="list-style-type: none"> <li>1. Request acknowledgment from administrator.</li> <li>2. Disconnect Users from PAM.</li> <li>3. Display message to Users (over login page).</li> </ol>
Re-Authenticate	<ol style="list-style-type: none"> <li>1. Request acknowledgment from administrator.</li> <li>2. Suspend User sessions.</li> <li>3. Display login request to Users (over login page).</li> <li>4. If authentication succeeds, restore suspended User session. If authentication fails, end session.</li> </ol>
Disconnect	<ol style="list-style-type: none"> <li>1. Request acknowledgment from administrator.</li> <li>2. Disconnect Users from target Device.</li> <li>3. Display message to Users.</li> </ol>
Record	<ol style="list-style-type: none"> <li>1. Request acknowledgment from administrator.</li> <li>2. Interrupt User sessions and start recording.</li> <li>3. Resume session to Users.</li> </ol>
Stop	<ol style="list-style-type: none"> <li>1. Request acknowledgment from administrator.</li> <li>2. Interrupt User sessions and stop recording.</li> <li>3. Resume session to Users.</li> </ol>

## **Display a Message to Users at Login**

This procedure describes how to configure a message containing important information to display in a dialog when a user logs in to the PAM UI. Examples of the type of information you might want to present in these messages include notifications about planned maintenance, availability of training for new available features, or process changes.

**Follow these steps:**

1. Log into the PAM UI.
2. Navigate to **Settings, Global Settings**.
3. Select the **Alerts** tab.
4. Set the **Show Informational User Message** option.
5. Use the text box and other related controls that appear to define your message and related settings.
  - Enter the message that you want to display in the text box. Limit: 64,000 characters.
  - Optionally, schedule when the message should be displayed using the following fields:
    - **Start Date:** The date when the message should start being displayed.
    - **Start Time (UTC):** The time when the message should start being displayed.
    - **End Date:** The date when the message should stop being displayed.
    - **End Time (UTC):** The time when the message should stop being displayed.
6. Select the **Save** button to commit your changes.

The following screenshot shows how to configure a message to warn users who log in on April 6 and 7 that PAM will be down for maintenance on the weekend:

☐ Show License Warning
 ☐ Show Recording Warning
 ☒ Show Informational User Message

PAM will be down for maintenance the weekend of April 8/9.

It will be available again on Monday April 10.

Start Date: 2023/04/06

End Date: 2023/04/07

Start Time (UTC): 00:00:00

End Time (UTC): 23:45:00

Reset Message Acknowledgement

**Reset Message Acknowledgments**

Once they have seen a message, users can select an option to acknowledge it so that it is not displayed on future logins. To reset user acknowledgments so the message is presented to *all* users when they next login, select the **Reset Message Acknowledgment** button.

**NOTE**

For information about the user experience, see [Accessing PAM](#).

## Maintenance

As an administrator, you can perform the Privileged Access Manager maintenance activities described in this section. This list of activities is not exhaustive. Some activities can be delegated to other administrators.

Use the table of contents to access the topics in this section.

## Configuration and Database Backups

To restore Privileged Access Manager instances for any reason, back up the configuration and database data. Backups are managed from the **Configuration, Database** UI page.

This topic explains:

### TIP

Schedule the database backups as soon and as frequently as practical. The backup is then available in case emergency recovery is needed.

### Types of Backups

As of version 3.3, database backups are performed in one step. Instead of copying the file and then compressing it, the file is compressed as it is copied. This method requires less disk space.

- **Configuration backup:** A configuration backup generates a file that contains all the unique settings and configuration information for each Privileged Access Manager instance. Use configuration files to roll back the configuration settings for a PAM instance. Use these files only on the server instance where they were created. This configuration file cannot be restored to or from another instance. The backup file includes the network context, globals, and settings such as "Disable Config User."

File-name format: gkyyyymmddhmmss.cfg

- **Database backup:** A database backup generates a compressed file that contains all the provisioning data, including:
  - Users and user groups
  - Devices and device groups
  - Socket and command filter configurations
  - Policies
  - Access data
  - Credential Manager data, with any A2A data

File-name format: gkdatabaseyyyymmddhmmss.gz; when downloaded, the *bin* extension is added

### Encryption of Configuration and Database Backup Files

The following information lists the encryption of configuration and database backup files.

### NOTE

Certificates, RSA authentication credentials, and cleartext passwords are not backed up.

- Scheduled configuration and database backup files are encrypted using AES-256-CBC, which is compliant with FIPS 140-2.
- Manual configuration backups are stored locally and encrypted using 3DES.
- Manual database backups are stored locally and not encrypted.
- Downloaded manual configuration backups are encrypted using 3DES.
- Downloaded manual database backups are encrypted using AES-256-CBC.

### NOTE

Beginning in version 3.0.1, only the appliance that performed the database backup can restore the database and function properly. Another appliance can restore the database, but it cannot decrypt the password data, so any functionality involving that data fails. To create a duplicate appliance for disaster recovery or migration purposes, see [Restore the Database to a New Appliance](#).

## Manual Backups

From the **Configuration, Database** window, a backup can be done manually. Select the **Save Database and Configuration** option. Separate files are created for the database and configuration data, and are stored on server hard drive.

File Type	File Name
Config	gk20170515211717.cfg
Database	gkdatabase20170515211715.gz

You can perform the following operations on these files:

- **Delete** - Delete the selected file from the hard drive.

### WARNING

**Warning!** This operation cannot be undone. Any deleted files are removed permanently.

- **Restore** - Restore the database or configuration file using the selected file. Restoring a file from a previously saved version overwrites any changes from the previous selected backup.
- **Download** - Copy the selected file from to your local hard drive. Downloaded files can be saved offline for long-term storage and retrieval.

## Scheduled Backups

You can schedule backups to occur automatically by selecting the **Backup Scheduler** option. Scheduled backups are offloaded to a specified external server. When you select this operation, the Backup Scheduler panel displays. If a backup schedule currently exists, the current schedule displays the month, day, weekday, and time of that scheduled backup.

For instructions on scheduling a database backup, see [Schedule a Backup of the Database](#).

## Export Backup Files

You can export backup files to an external location, protecting them in case you must restore a configuration.

Use one of the following methods to export a backup file:

- **Manually** - from the Database page, select the file from the list and select **Download**. If no files are listed, select **Save Database and Configuration**.
- **Automatically** - use the Backup Scheduler and specify the location for the backup file in the **Share Path** field.

### NOTE

- [Restore the Database from a Backup File](#)
- [Reset the Database to the Factory Defaults](#)
- [Compact the Database to Regain Storage Space](#)

## Schedule a Backup of the Database

You can schedule backups to occur automatically by selecting the **Backup Scheduler** option. Scheduled backups are offloaded to a specified external server. When you select this operation, the Backup Scheduler panel displays. If a backup schedule currently exists, the current schedule displays the month, day, weekday, and time of that scheduled backup.

This page contains the following sections:

- [Configure a Backup Schedule](#)
- [Use Your Own Public Keys for SCP and SFTP File Transfers \(Optional\)](#)
  - [Create the Target Application.](#)
  - [Create the Backup Target Account.](#)
  - [Schedule a Backup Using the Backup Target Account.](#)

## **Configure a Backup Schedule**

To schedule a database backup, follow these steps:

1. Select **Configuration, Database.**
2. Select the **Backup Scheduler** tab.  
In the scheduler, the current schedule is displayed. If a scheduled is already configured, the pane displays the schedule entries.
3. Populate the schedule fields. Most fields are self-explanatory. For the **Protocol** field, SCP and SFTP send files using these SSH-based protocols. NFS, CIFS, and Amazon S3 write to file mounts. Select **Mount** at the bottom of the page to mount the file.
  - **SCP** and **SFTP**: Set the **Share Path** in the form `/path` . Enter a **Port**, and select a **Backup Target Account**. See [Use Your Own Public Keys for SCP and SFTP File Transfers](#) for instructions on setting up a Backup Target Account.

### **NOTE**

(SCP and SFTP only). In clustered implementations of 2.x versions of the product, you could specify different backup servers for each node. In 3.x implementations, you specify a single backup server for the entire cluster. However, you can specify a different *directory* in the share path for each node. For example, `Server1/backupNode1` and `Server1/backupNode2` .

- **NFS**: Set the **Share Path** in the form `/<path_on_server>` . Enter a **Hostname** as FQDN or IP address. (Optional) Enter a non-default **Request Timeout** value (in tenths of a second). If no value is specified, the default is determined by the NFS server, typically 600.

### **WARNING**

Do not use the same NFS mount point that you are using for [session recordings](#). The session recording and scheduled database backup processes create and delete a file with the same name to check the remote storage status. If you specify the same NFS mount point, file locking can occur as both processes attempt to create or delete the same file.

- **CIFS**: Set the Share Path in the form `\\<hostname>\<share>` . Enter a **User Name** and **Password** to access the share account. Enter the **Domain**. Select the **SMB Version** (Server Message Block) used by the target system. Newer versions of SMB are more secure. If you do not support older file shares (like Windows 2003), use SMB2 or SMB3, provided the CIFS system supports it.
  - **Amazon S3**: Select the AWS S3 **Bucket** and the **AWS Provision**, as set in **Configuration, 3rd Party, AWS, AWS Configured Connections, Access Key Alias** – Region combination.
4. Complete the additional fields for the option that you select.
  5. (For SCP or SFTP protocols only.) Establish a secure communication that does not require an interactive login:
    - a. Download the key files from the public key file.
    - b. Copy these key files to the destination server, into the home directory of the user who represents Privileged Access Manager for authentication.
    - c. In the `.ssh` directory of the destination server, import or append the contents of the key files into the **authorized\_keys** file. If an `authorized_keys` file does not exist, create one.
    - d. Verify that the following directory and file permissions are applied or the backup fails:

- **.ssh directory**: owner has read (r), write (w) and execute (x) permissions
  - **authorized\_keys** file: owner has read (r) and write (w)
6. (Optional) Select **Delete After Successful Send** to remove the backup files from local storage on the PAM server.
  7. Set the **Maximum Files to Keep Locally** to specify the number of backup files that are stored locally on the server. Scheduled backup files are available for download in the file operations area. This field refers only to the local storage of backup files. The backups on an external storage device must be managed outside of Privileged Access Manager.
  8. Select **Save Schedule** to set the backup

### **Use Your Own Public Keys for SCP and SFTP File Transfers (Optional)**

You can use your own generated public keys for backup file transfers over SCP and SFTP connections, using the following process:

1. [Create the Target Application.](#)
2. [Create the Backup Target Account.](#)
3. [Schedule a Backup Using the Backup Target Account.](#)

Complete these steps in the UI.

#### **Create the Target Application**

To create a **CAPAM\_DatabaseBackup** target application, perform the following steps:

1. Select **Credentials, Manage Targets, Applications**.  
The Target Applications list appears.
2. Select **Add**.  
The Add Target Application window appears.
3. Select the magnifying glass next to the **Host Name** field and pick the host system to which your database files are to be backed up.
4. In the Application Name field, enter **CAPAM\_DatabaseBackup**. If the Target Application name is anything else, the Scheduled Backup does not work.
5. Select the "UNIX" **Application Type**.
6. Select **OK** to save the Application.

#### **Create the Backup Target Account**

To create a backup target account that uses the target application, complete the following steps:

1. Select **Credentials, Manage Targets, Accounts**.  
The Target Accounts list appears.
2. Select **Add**.  
The Add Target Account window appears.
3. Select the magnifying glass next to the **Application Name** field and select **CAPAM\_DatabaseBackup** from the Target Applications list that appears.
4. Specify a unique name for the target account in the **Account Name** field.
5. Select the "SSH-2 Public Key Authentication" **Protocol** option.
6. Do one of the following steps to specify a public key to use:
  - Select the key icon next to the **Private Key** field to generate a key pair.
  - Copy your own key pair into the **Public Key** and **Private Key** fields.
7. Select **OK** to save the Account.

#### **Schedule a Backup Using the Backup Target Account**

To schedule a backup on the target database backup system, use the backup target account and perform the following steps:

1. Select **Configuration, Database**.
2. Select **Backup Scheduler**.
3. Configure the Schedule and Protocol options according to [Configure a Backup Schedule](#).
4. Select your backup target account: next to the **Backup Target Account** field, choose the **Select** button (icon of a magnifying glass) to display the **Database Backup Target Account** selection panel. Use this panel to select your backup target account.

After you select a target account, the **Backup Target Account Device** field displays the name of the device that is associated with the target account you selected.

#### NOTE

If you no longer want to use the **Backup Target Account** for your backup, select the **Clear** button (icon of a circle with a line) to remove the account from the field.

5. Select the **Download** button to download the public key file to the home directory of the user account that represents Privileged Access Manager for authentication.
6. Navigate to the `.ssh` directory. Append the contents of the public key file into the `authorized_keys` file. If the `authorized_keys` file does not exist, create one.
7. Select **Save** to save the schedule.

## Restore the Database from a Backup File

You can restore the server configuration or database from existing backup files.

Restoring these files has the following consequences:

- The instance reverts to an earlier state, including passwords.
- The server overwrites all session logs. However:
  - Immediately before recovering or restoring, you can save and download the logs.
  - Before a recovery/restoration is required, you can use the external log server option.

Restoring the configuration does not interfere with session recordings. Session Recordings are saved externally, so access to this data is maintained.

The red highlighted text indicating a violation within recordings is lost for the interval after the database was last saved. (This highlight is not available for RDP graphical session recordings.)

During the restoration process, the PAM server compares the existing database size to the size of the backup file.

- If the existing database size is greater than the size of the backup file, the restoration completes.
- If the backup file is larger than the existing database, the server determines whether 100 MB exists within the file system. If not, the restoration fails.
- The next calculation determines whether the size of the backup file is more than half the available disk space. If it is less than half the available disk space, the restoration succeeds. If it is greater than half the available disk space, the restoration fails.

To restore the entire system, see [Recover the Hardware Appliance](#).

#### NOTE

Beginning in version 3.0.1, only the appliance that performed the database backup can restore the database and function properly. Another appliance can restore the database, but it cannot decrypt the password data, so any functionality involving that data fails. To create a duplicate appliance for disaster recovery or migration purposes, see [Restore the Database to a New Appliance](#).



## **Restore the Database**

1. Navigate to **Configuration, Database**.
2. In the **Database** tab, select the file and select **Restore**. (See [Configuration and Database Backups](#) for file descriptions.)  
If the configuration or database file does not appear in the list, upload a saved backup. On the **Upload File** tab, select **Choose File** to select the database file, select the file, then select **Upload**. A copy of the backup is now available.
3. Select **Restore**, then select **OK** in the confirmation pop-up window to begin restoration.
4. After restoration completes, the server automatically reboots.
5. Close your browser, then restart it, and log in as *super*.

## **Reset the Database to the Factory Defaults**

1. Navigate to the **Configuration, Database** screen.
2. From the Database tab, select **Reset** to reset configuration to the factory default values.
3. After reset completes, the server automatically reboots.
4. Close your browser, then restart it, and log in.

## **Compact the PAM Database to Improve Startup Time**

Compact the PAM database to increase available storage space and improve startup time by purging space that is allocated to entries that have since been deleted. If you need to compact the database frequently, you should consider adding more storage space.

### **NOTE**

Users cannot log on while the database is compacting. To avoid this disruption in service, compact the database only during a planned maintenance window.

### **NOTE**

The procedures in this content assume that you are running a PAM cluster. If you have a single-server deployment, ignore cluster-specific directions.

## **Prepare to Compact the Database**

To prevent activity against the database during compaction, complete the following steps:

1. Turn on Maintenance Mode on each node in the cluster to prevent new logins.
  - a. Navigate to **Configuration, Diagnostic, System**.
  - b. Set the **Maintenance Mode** option to **On**.
2. Turn clustering off.  
On the primary master node, navigate to **Configuration, Synchronization**. In the **Cluster Settings**, select **Turn Cluster Off**.
3. (Optional) Log out current user sessions. Although Maintenance Mode prevents new logins, it does not disconnect current user sessions. You can force disconnections using the **Manage Sessions** screen:
  - a. Navigate to **Sessions, Manage Sessions**.
  - b. Select any entry in the table and select **LOGOUT** above the table. You can log out any users (except yourself).
4. If the Credential Manager External CLI is enabled, follow these steps on the primary master to disable it.
  - a. Select **Settings, Credential Manager** to access the Credential Manager settings.
  - b. Clear the **Enable External CLI** checkbox.
  - c. Select **Save**.
  - d. Restart the instance



## Compact the Database

After user activity has ceased on the master node of the primary cluster site, compact the database.

**Follow these steps on the primary master:**

1. Go to **Configuration, Database**.
2. From the **Database** tab, select **Compact**.

### NOTE

The **Compact** button is only active when Maintenance Mode is on and clustering is inactive.

A dialog stating that database compaction can take a long time appears.

3. Select **YES** to continue. The duration of the process and the amount of space that is freed depend on the number of entries deleted. To stop the process, select **Cancel**.

## Restore Your Environment After Compacting the Database

To bring your environment back up after compacting the database, complete the following steps:

1. Turn off Maintenance Mode on each node in the cluster to allow new logins.
  - a. Navigate to **Configuration, Diagnostic, System**.
  - b. Set the **Maintenance Mode** option to **Off**.
2. If applicable, follow these steps on the primary master to enable the Credential Manager External CLI.
  - a. Select **Settings, Credential Manager** to access the Credential Manager settings.
  - b. Set the **Enable External CLI** option.
  - c. Select **Save**.
  - d. Restart the instance
3. Turn clustering on.

On the primary master, navigate to **Configuration, Synchronization**. In the **Cluster Settings**, select **Turn Cluster On**.

### NOTE

Once the cluster is back up, the compacted database is propagated to all other cluster members.

## Restore the Database to a New Appliance

Beginning in version 3.0.1, only the appliance that performed the database backup can restore the database and function properly. Another appliance can restore the database, but it cannot decrypt the password data, so any functionality involving that data fails. The backup requires the key encryption key from the original appliance for restoration. This requirement prevents a bad actor from getting access to a database backup so that the passwords can then be decrypted and compromised.

To create a duplicate appliance for disaster recovery or migration purposes, follow these steps:

1. Deploy a Privileged Access Manager appliance. See [Deploying](#) for instructions.
2. Join the original appliance in a cluster with the new appliance, configuring the new appliance as a member of a secondary site. See [Set Up a Cluster](#) for details on how to configure clustering.  
You now have a "live" backup of the data from the original appliance because all cluster data is replicated to all nodes in the cluster. For disaster recovery, this new appliance should be in a different data center
3. If you want a new, independent appliance, the new appliance can [Cluster Synchronization, Promotion, and Recovery](#) for details. The new appliance and the original appliance can then move forward in separate, distinct, environments.

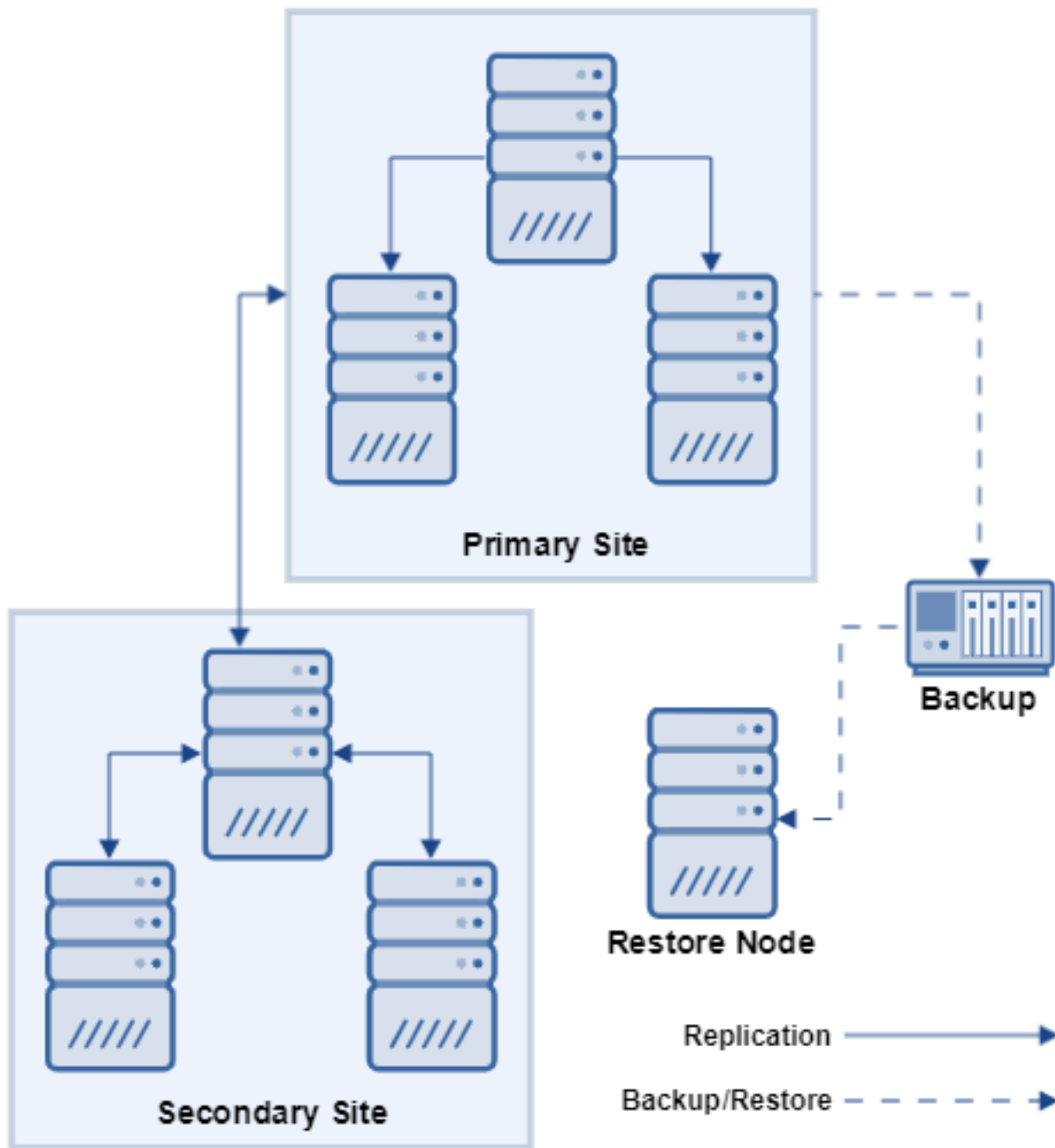
### NOTE

- [Cluster Backup and Disaster Recovery Process](#)

## Cluster Backup and Disaster Recovery Process

Beginning in version 3.0.1, only the appliance that performs a database backup can restore the database and function properly. Another appliance can restore the database, but it cannot decrypt the data unless it uses the same key encryption key (KEK) that was used when the backup was taken. PAM members all begin with a unique KEK. When members are joined to a non-HSM cluster, they inherit the KEK of the cluster leader. If you do not have the latest KEK, then any functionality involving data decryption fails and your appliance may become unusable. The backup requires the latest KEK for restoration. This requirement prevents a bad actor from getting access to a database backup to decrypt and compromise passwords.

A cluster is effectively a living backup of the database. Each member of a multi-master or primary site has the entire database. If you have secondary sites, they can be promoted to primary sites. But what happens if the entire cluster is lost in a disaster? The secure backups that you make can only be restored to a member of the cluster. One way to protect against this scenario is to create a stand-alone cluster member to restore the database in an emergency.

**Figure 62: Cluster Restore Member**

**To set up a stand-alone member backup, follow these steps:**

1. During the initial setup of a PAM cluster, add an extra member to the cluster. If the cluster already exists, you can subscribe a new PAM instance to join it.
2. After all members of the cluster are in sync, log in to the extra member and remove it from the cluster.
3. 1. Go to **Configuration, Clustering**, and select **Leave Cluster**.

This member is now a stand-alone PAM instance and has the same encryption key sets as the other cluster members. If all members of the cluster are unavailable, this “restore node” can restore a backup of a cluster database.

2. Remove this member from the network.
  4. Select a member of the Primary Site to perform a daily backup.
    - a. Go to **Configuration, Database, Backup Scheduler**. See [Schedule a Backup of the Database](#) for details.
    - b. **Save** the database backup schedule.
- The DB and configuration are backed up to external storage.

**To recover the backup using a stand-alone member, follow these steps:**

1. Access the “restore node.”
2. Load the latest database and configuration backup from the external storage. See [Restore the Database from a Backup](#) for instructions.
3. Use this node as the first member of a new Primary Site to set up a new cluster.

## Hardware Appliance Backup and Recovery

A backup of the PAM hardware appliance copies the OS, the software, and the configuration data. The backup also copies the provisioning data of managed users and devices. Use a backup to protect against software loss and to roll back the system to a known good state.

You can perform the following tasks:

### NOTE

Backups of the PAM databases and configurations are not covered in this topic. For information about database backups, see [Configuration and Database Backups](#).

You can perform a system backup only for the hardware appliance, not for an OVA or an AWS AMI instance. For information about AWS AMI backups, see [AWS AMI Backup and Recovery](#)

### Appliance Backup

An appliance backup copies system data from the primary drive to the backup (secondary) drive. During a backup, the previous version is written over with the new one so that only the most recent backup is ever in storage. This backup cannot be exported. To protect settings and data, export configuration and database backups.

You can complete a backup using the following methods:

- Manually, when you use the feature **Backup Appliance**.
- Scheduled, which results in automatic backups. Use a scheduled backup for every hotfix installation that requires a reboot, and every upgrade. You do not have to perform a backup manually in advance.

### Appliance Recovery

An appliance recovery restores the appliance from a backup of the appliance. The recovery returns the system back to the previously saved state.

Perform a recovery when:

- The system or firmware malfunctions or fails.
- A firmware upgrade appears to initiate problems.

### NOTE

If the PAM Server software fails to boot, you can reset the appliance back to its factory default state. For more information, see [Reset the Appliance to Factory Default State](#).

Hardware appliance backup and recovery are performed from the **Configuration, Upgrade** page.

Use the table of contents to access the topics in this section.

## Backup the Hardware Appliance

A backup of the hardware appliance creates a single copy of the current state of the appliance. The last saved software is copied from the primary drive onto the backup solid-state drive (SSD) to the last saved version. If the system malfunctions or fails, use the backup to recover the system. You can also use the backup to restore the system after the installation of a firmware package, such as a release upgrade or hotfix.

### TIP

The best practice is to perform system backups only during an installation or maintenance window.

These characteristics apply to system backups:

- A single backup is maintained – The secondary drive stores up to an entire primary drive capacity. The drive can contain only the most recently executed backup.
- Upgrades are done in the background – As part of any hotfix that requires a reboot or any upgrade, Privileged Access Manager performs the backup process automatically and silently.
- A full copy of the primary drive is made – During the backup process, the secondary drive makes a complete copy of the primary drive.
- Reboots the system automatically – After copying the primary drive, the system automatically reboots.

### Follow these steps:

1. Log in to the UI.
2. If this appliance is part of a synchronized cluster, turn off the synchronization.
3. Navigate to **Configuration, Upgrade**.
4. Select the **Backup & Recovery** tab.
5. From the **Backup & Recovery** tab, select **Perform Full Appliance Backup**.
6. At the confirmation prompt, select **Proceed**.  
A red text message displays asking you to wait.  
When the backup completes, the appliance automatically reboots.
7. At the login page, log in and navigate back to the Upgrade page.  
A successful backup generates a message in the Backup Appliance panel identifying the date and time of the backup.

The backup is complete.

## Recover a 404L Hardware Appliance

Learn how to recover a 404L hardware appliance from the last backup you performed to return it to its previous state. This topic describes how to recover the hardware appliance from the user interface or a serial cable.

### WARNING

Perform a system recovery only when recommended by Broadcom Support.

### Recover the Appliance Using the User Interface

If the appliance becomes inaccessible from the network, recovery is also possible from the Console in coordination with Support.

### NOTE

After this procedure, the appliance automatically reboots. To avoid impacting a production environment, perform this action only during an installation or maintenance window.

**Follow these steps:**

1. Log in to the UI.
2. If the appliance is part of a synchronized cluster, do the following steps to turn off the cluster:
  - a. Select **Configuration, Clustering**.
  - b. In the Cluster Settings, select **Turn Cluster Off**.
3. Navigate to **Configuration, Upgrade**.
4. Select the **Backup & Recovery** tab.
5. Select **Recover Appliance from Latest Backup** to start the process.
6. When you see the confirmation prompt, select **Proceed**.  
A red text message displays asking you to wait.  
When the recovery completes, the system reboots automatically, eventually refreshing with the login page.
7. Log in, and navigate to the **Upgrade** page to confirm recovery.  
If the recovery succeeded, the previous backup message no longer appears in the **Backup Appliance** panel.

**Recover the Appliance Using a Serial Cable**

PAM physical appliances have two solid-state drives (SSDs):

- A **Primary** drive that contains the current, operational PAM image.
- A **Secondary** drive that contains one or more backup images. (Any installation patch that requires a reboot writes a new backup image.)

**CAUTION**

PAM can only revert to an image on the secondary drive. Be careful not to overwrite a recovery image that you want to maintain.

Before you begin, locate an RS232 to RJ45 serial cable, and connect one side to the PAM console and the other side to your laptop. You should have one console cable that was shipped with the physical appliance, such as the one shown in the following image:

**Figure 63: RS232 to RJ45 serial cable**

**Follow these steps:**

1. Power down the unit.
2. Connect the serial cable to the RJ45 socket marked **Console** to a computer where you have a console-viewing client.

3. Launch putty (or other terminal emulator program) and configure the following settings:
  - **Connection speed:** 115; 200
  - **Data bits:** 8
  - **Stop bits:** 1
  - **Parity:** None
4. Start the appliance.
5. During the boot process, press and hold the **Esc** key within 5 seconds to open the boot loader menu.
6. Use the **^** and **v** keys to select the last entry in the GRUB menu (the latest PAM backup image, of the form "CA PAM x.x.x.x Backup as of Date Time").
7. Press **Enter**.

The boot loader initiates the recovery operation, performing the following steps without further intervention:

1. Boots PAM from the secondary drive.
2. Copies the selected PAM backup image from the secondary drive to the primary drive, replacing the corrupted image.
3. Boots PAM from the restored image on the primary drive.

#### NOTE

The recovery operation may take a considerable amount of time.

## Reset the Appliance to Factory Default State

This topic describes how to reset the PAM 404 hardware appliance to its factory default state if the PAM application repeatedly fails to operate effectively after you have attempted all other recovery methods.



#### CAUTION

The factory reset function wipes all database entries and any upgrade patches applied since the PAM version originally installed on the appliance. For this reason, we recommend that you only use the factory reset function if advised to do so by Broadcom Support.

Topics in this content:

### Reset the Appliance to Factory Default Settings

This section describes how to reset the appliance to its factory default settings.

#### Follow these steps:

1. Locate the hole indicated by the red arrow in the following photograph of the PAM 404 appliance.

**Figure 64: Photograph of the appliance showing the recessed Factory Reset button.**



#### NOTE

Not all PAM 404 hardware appliances have the "Reset" label printed beside the hole for the recessed **Reset** button. In either case, the recessed button provides the same factory reset action.

2. Straighten a paperclip or locate another object of similar dimensions.
3. Insert the straightened paperclip (or alternative object) into the indicated hole and press and *hold* the recessed Factory Reset button for at least 3 seconds.

The appliance resets to its factory settings and the display shows the following message "System is booting... LOM card not existed".

### **Restore the Appliance to Its Previous State**

Do the following procedures to restore the appliance to the state it was in when the last good backup was taken:

1. **Configure Network Connections for the Appliance:**

After the appliance comes back up after the factory reset, configure the IP network interfaces so the appliance can access a network. You can set up your network connections using the LCD panel, the CA PAM UI, or a Console port. The appliance is inaccessible to the network until its IP address is assigned. For more information, see [Configure Network Connections for the Appliance](#).

2. **Reinstall Service Packs and Hotfixes:**

To restore the appliance to its previous release state, reinstall all service packs and hotfixes that were previously installed when the database was last backed up.

3. **Restore the Database from a Backup File:**

To restore the configuration and database data to your appliance, restore the database from a backup file. For more information, see [Restore the Database from a Backup File](#).

## **AWS AMI Backup and Recovery**

To protect from software loss, backup Privileged Access Manager deployed on an AWS AMI instance. The procedure backs up the entire instance, allowing you to roll back all software to a known good state.

### **Back Up the AMI Instance to a Volume**

The AWS AMI backup process creates a snapshot of the state of the current instance. It stores the snapshot in the designated S3 bucket for later use in recovery.

#### **TIP**

This procedure can be automated by using the AWS API.

#### **Follow these steps to backup the instance:**

1. Navigate to your AWS Management Console EC2 view.
2. From the **Navigation** panel, select **INSTANCES, Instances**.  
If needed, search for the instance Name or instance number (labeled "Instance").
3. From the Instance list, select the checkbox of the instance you want to back up.
4. From the **Instance Actions** menu, select **Stop** to stop the instance to freeze its state.

#### **NOTE**

When in a production environment, stopping the instance might not be practical.

5. Record the **Instance ID**.
6. From the Navigation panel, select **ELASTIC BLOCK STORE, Volumes**.
7. Identify the volume that is attached to the instance you want to back up.  
To more easily find the volume, select the arrow in the **Attachment Information** column heading to reorder the entries alphabetically to find the Instance ID.
8. Select the checkbox of this volume.



9. From the **More** drop-down list, select **Create Snapshot**. In the pop-up that opens, enter a **Name** and optionally, a **Description**.
10. Select **Yes, Create**. Ensure that this snapshot is created in the same instance zone.
11. Go back to the Navigation panel, and select **ELASTIC BLOCK STORE, Snapshots**.  
You see an entry for your snapshot, which might still be generating. This snapshot is your full system backup for this point in time.
12. Make a note of the **Snapshot ID**, especially if your snapshot Name or Description does not provide identifiable information as to when and why the snapshot was created.  
You might also want to create extra snapshots at other points in time. You are not limited in the number of snapshots.
13. Create a volume from the snapshot.

### **Create the Volume from the Snapshot**

Use the snapshot to restore the instance to this state. Privileged Access Manager cloud instances are available in the AWS environment. Within this environment, you can create a snapshot of an instance at a specific time, and then recreate it if an instance failure occurs.

Recover a volume from a snapshot of a previous machine state that is stored in a designated S3 bucket. This volume can then be substituted for the non-functioning volume.

#### **Follow these steps:**

1. Navigate to your AWS Management Console EC2 view.
2. From the **Navigation** panel, select **INSTANCES, Instances**.
3. Find the correct instance and record the **Instance ID**. If necessary, stop the instance.
4. Return to the **Navigation** panel and select **ELASTIC BLOCK STORE , Snapshots**.
5. Locate and select the checkbox of the correct snapshot. Record the snapshot ID for later use.
6. From the top-level buttons in this panel, select **Create Volume** and give the recovered volume a **Size** that is equal or larger than the original.

### **Restore the AMI Instance from the New Volume**

After you complete the following procedure, the machine ID changes. A license update that reflects that change is required.

1. Return to the **Navigation** panel and select **ELASTIC BLOCK STORE, Volumes**.
2. Confirm that the recovery volume exists by checking for the snapshot ID in the generated Volumes list. To locate the volume instance easily, reorder the Snapshot list alphabetically for the correct **snap-xxxxxxx** number.  
It is not attached to a machine instance at this point. You can tell because the **Attachment Information** field is blank.
3. Find the old volume that you want to replace. This volume *is* attached to the machine Instance ID and is in the **Attachment Information** column.  
To more easily locate the attached volume, reorder the **Attachment Information** list and scan according to the instance number.
4. Select the checkbox of this old volume that you want to remove.
5. From the **More option**, select **Detach Volume**.  
This can take a few minutes. Select **Refresh** to confirm completion.
6. Select the checkbox of the volume you want to use for recovery.
7. Select **Attach Volume**. In the Attach Volume page, select the Privileged Access Manager **Instance**. In the Device field, enter **/dev/sda**.
8. If necessary, restart the instance. From the **Navigation** panel, select **INSTANCES, Instances**.

## Mitigate Host Header Attacks

Privileged Access Manager can mitigate host header attacks by denying any X-Forwarded-Host values that are not specified in a whitelist. This feature then protects against arbitrary and invalid hosts headers.

**To configure this defense, perform these steps:**

1. Go to **Configuration, Exceptions**.
2. Add the Whitelist Hosts to the text box under PAM Exception Rules. Separate the entries with commas or put them on new lines.
3. Select **Save**.
4. Go to **Configuration, Security, Access**.
5. On the **X Forwarded Host Check** line, select **Enabled**.

The X-Forwarded-Host Check is now enabled. Only **X-Forwarded-Host** HTTP headers that are specified on the Exceptions page are accepted by Privileged Access Manager.

## Memory Management

PAM appliances allocate memory according to their amount of available RAM. Two new configuration files (one each for primary and secondary site members) control the allocation. If you are experiencing “Out of Memory” errors or performance issues, contact Broadcom Support.

### Memory Management

This chart shows the default memory allocation to major processes in the PAM appliance according to its total amount of RAM:

Appliance memory in GB	Tomcat memory in MB	JBoss memory in MB	PHP memory in MB	MySQL buffer pool in MB	Hazelcast thread count
4 or less	1536	1024	512	128	1
8	1638	1092	546	1024	53
12	2457	1638	819	1536	79
16	3276	2184	1092	2048	106
20	4096	2730	1365	2560	133
32	6552	4368	2184	4096	213
48	9828	6552	3276	6144	326
64	13104	8736	4368	8192	426

## View System Information

The **System Info** pane provides administrators with system status and version information on five tabs.

### Basic Info Tab

The **Basic Info** tab includes your version, and several status indicators:

- **Version** indicates the detailed version number of your appliance or instance.
- **FIPS Mode** indicates whether you are running in FIPS mode.
- **HSM** indicates the status of a hardware security module (HSM). The following values are possible

- SafeNet LUNA Network HSM
- SafeNet LUNA PCI-E
- Entrust nShield Connect
- None
- Licensed, not Configured

For more information about HSMs, see the [Hardware Security Modules \(HSMs\) for Credential Manager](#) section.

- **TLS v1.0/1.1** indicates whether these communication protocols are enabled or disabled through the **TLS v1.0/1.1 Connection Allowed** option.
- **RDRAND** indicates whether the RDRAND hardware random number generator is available.
- **Cryptographic Provider** indicates whether HSM, OpenSSL, WolfSSL, or Bouncy Castle is being used.

### System Resources Tab

The **System Resources** tab displays current CPU usage; total, used, and free disk storage; and total, used, and available memory.

#### NOTE

If you resize your disk in VMware, AWS, or Azure, it is reflected here and in the Appliance Status on the **Dashboard Overview Tab**. Follow the resizing procedure for your platform, then reboot your instance. Go to **Configuration, Power**, and select **Reboot Instance**. For information about resizing VMware or AWS disks, see [Deploy a VHD on Azure](#).

### System Activity Tab

The **System Activity** tab displays information about general system activity and status information about session recording reconciliation processes on the *current node*:

- **General System Activity**
  - **Uptime**: The amount of time that the server has been up since the last appliance boot,
  - **Active Logins**: The number of users that are currently logged in
  - **Active Sessions**: The number of active connection sessions.
- **Session Recording Reconciliation Process Status**:
  - **Most Recent Recordings**: Status of the job that reconciles recent session recordings.
  - **Restored Recordings**: Status of the job that reconciles session recordings that are recovered from archives.
  - **All Other Recordings**: Status of the job that reconciles all other recordings.

If reconciliation is operational, the status of each reconciliation job is one of following values:

- **Available**: The reconciliation process is idle.
- **Running**: The reconciliation process is in progress.

If reconciliation is not operational, all reconciliation jobs report the same one of the following failure reasons:

- **Unmounted**: The reconciliation process cannot run because the session recording share is not mounted.
- **Mount Not Available**: The reconciliation process cannot run because, although the session recording share is mounted it is not reachable, probably because of a network outage.
- **Maintenance Mode**: The reconciliation process cannot run because the node is in maintenance mode.
- **Health Check Failed**: The reconciliation process cannot run because the node failed a [health check](#).

#### NOTE

For more information about session recording reconciliation, see [Configure and Manage Session Recording](#).

### **Licensing Tab**

The **Licensing** tab lists the number of devices that are allowed with your license, and the number in use, in the form of Devices used/Devices licensed. Each type of license, such as Password Management and A2A are listed. Licensed capabilities are also listed, such as Mainframe, Threat Analytics, and External API.

### **Hardware Identifiers Tab**

The **Hardware Identifiers** tab displays the Hardware ID and the Hardware Serial Number (if assigned).

### **Hotfixes Tab**

The **Hotfixes** tab identifies any hotfixes that are applied to this installation of Privileged Access Manager.

### **General Tasks**

You can perform the following tasks from any tab:

- To refresh the data in the **System Info** pane, select the Refresh circular arrow icon in the upper right of the pane.
- To download a text file of the data in the **System Info** pane, select the Download checkmark icon in the upper right of the pane.

## **Cluster Maintenance**

This content describes best practices for maintaining your cluster.

### **Routine Cluster Maintenance**

Administrators should regularly log into the appliance to monitor the various health information available on the **Dashboard Overview Tab**. A summary of conditions of which you should be aware, including the following information appear at the top of the page:

- Health alerts on the cluster members
- Configuration warnings (configuration password has not been changed, users are being monitored by the TAP server, and so on.)
- Operational warnings (maintenance mode is on, primary or secondary session recording mounts are down, insufficient disk space for network backups, and so on).

The **Dashboard Overview Tab** also reports CPU usage and disk usage for each node in the cluster. Causes of high disk utilization include the following issues:

- Many locally stored database backups
- Failure to prune the metrics or logs tables in the database.
- Leaving logging levels elevated for a prolonged interval

### **Best practices for Backups**

You can perform database and configuration backups at any time. They can be run manually or invoked on a fixed schedule. Backups can be stored on the appliance or remotely. Remote copies can be made manually or automatically. For more information, see [Configuration and Database Backups](#) for details.

#### **NOTE**

Restoring a backup to an appliance that was not part of the original cluster results in scrambled passwords. This situation is caused by a security enhancement that specifies to which appliances a backup can be restored. To address this issue, follow these steps:

1. Subscribe the target appliance to the cluster as a secondary site while in maintenance mode.
2. Unsubscribe the appliance.

3. Restore the database.

### **Best Practices for Live Migration and Live Snapshots of Sites Running on VMware vSphere**

You can take a live snapshot of secondary nodes at any time.

#### **WARNING**

Do not take a live snapshot of the primary node while the cluster is live. Doing so may drive the nodes out of sync.

#### ***VMware vMotion Support For Live Migration***

PAM supports VMware vMotion for live migration of both primary and secondary cluster members running on VMware vSphere.

#### **NOTE**

Do not attempt to simultaneously move all or most primary members, which may result in a cluster warning, a potential quorum loss, or both. PAM attempts to self-heal all warnings. However, if they do not heal successfully, you may need to perform a manual sync. PAM continuously evaluates quorum and automatically attempts to recover from a quorum loss.

#### ***VMware DRS or Live Snapshotting Support***

PAM does not support the use of VMware DRS, or other functionality relying on live snapshotting on a PAM VM that is a *member of a live cluster*. However, you can perform live snapshotting with the cluster up and running using the following procedure.

#### **Follow these steps:**

1. Remove a single PAM VM from the cluster, typically a secondary node.
2. Snapshot the PAM VM that you removed from the cluster.
3. Resubscribe the PAM VM back into the cluster.

### **Save the State of a Physical Appliance**

To save the entire state of a physical appliance, use the **Perform Full Appliance Backup** operation. A full appliance backup is distinct from a database backup; it writes the entire contents of the primary drive onto the secondary drive. Only one full appliance backup can be kept on the secondary drive so each full appliance backup wipes out any previous backup. You cannot download a full appliance backup from the physical appliance.

#### **NOTE**

This operation forces a reboot, throwing all users off the system. Perform it only during scheduled downtime.

#### **Follow these steps:**

1. Turn off the cluster.
2. Put the first node of the primary site into maintenance mode.
3. Open the **Configuration, Upgrade** page **Backup & Recovery** tab and select **Perform Full Appliance Backup**. The current state of the primary drive is copied onto the secondary drive and the appliance reboots.
4. Sign back on and turn off maintenance mode.
5. Turn on the cluster.

#### **Follow these steps to restore the appliance to the backed-up state:**

1. Turn off the cluster.
2. Turn on Maintenance Mode.
3. Open the **Configuration, Upgrade** page **Backup & Recovery** tab and select **Recover Appliance From Latest Backup** button.

4. Turn on the cluster.

The contents of the secondary drive are restored to the primary drive and the appliance reboots.

## Credential Manager Reports

You can generate reports from Credential Manager data. Credential Manager stores audit, metric, and event data in the database. Using this data, Credential Manager can produce four types of reports: activity, metric, SQL, or command.

- **Activity:** Pulls data from the auditlog table in the Credential Manager database. These reports are not customizable. An example is the Administrative Activities report.
- **Metrics:** Pulls data from XML blocks within entries in the metrics table of the Credential Manager database. All entries are available to the report. These reports can be customized. An example is the Account Request report.
- **SQL:** Generates reports by executing SQL queries on the database. These reports can be customized. An example is the Orphaned Request Server report.
- **Command:** Pulls data from CLI search command responses.

Credential Manager can produce a defined set of reports using these report types. The reports reflect the time zone that the user selects or UTC. All reports are based on Coordinated Universal Time (UTC). You can customize metrics and SQL reports to produce more reports.

### NOTE

Credential Manager uses pop-ups to display reports. Some web browsers might block pop-ups. We recommend that you configure your browser to allow all pop-ups.

Use the table of contents to access the topics in this section.

## Available Credential Manager Reports

The following list describes the available Credential Manager reports. The maximum number of report entries defaults to 5000. For information about changing this setting, see Maximum Number of Report Entries on [Set Up Credential Manager Operation Settings](#). The setting can be changed at **Settings, Credential Manager, General Settings**.

You can refine the output of most reports by date and other filterable parameters by entering values in the available fields or selecting values using the calendar or magnifying glass icons beside them as is seen in the following screenshot:

**Figure 65: Credential Manager report filters**

**Report: Account Passwords Update Attempts**

Description: Lists accounts where an attempt to change the password was made

Time Zone: UTC

Quick Dates:

Start Date:

End Date:

Target Account Name:

Changes By: dax axelrod

Target Server Host Name:

Target Application Name:

Account Access Type:

Password View Policy ID:

Attempts: ☒ All ☐ Changes ☐ Failures

Output Format: ☒ HTML ☐ CSV ☐ PDF

OK CANCEL

The following content lists the data returned by all the available reports and indicates which values can be filtered when requesting the report:

### ***Account Password Update Attempts***

This report lists accounts where an attempt was made to change the password. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or the **Start** and **End Date** of the update. (Filterable)
- **Target Account Name:** The name of the target account. (Filterable)
- **Changes By:** The User who initiated the password update attempt. (Filterable)
- **Target Server Host Name:** The name of the target server host. (Filterable)
- **Target Application Name:** The name of the target application. (Filterable)
- **Account Access Type:** The type of account access. (Filterable, **but not included in the report**)
- **Password View Policy ID:** Use the magnifying glass to filter by Password View Policy. (Filterable, **but not included in the report**)
- **Changed:** This value displays TRUE if the password update attempt succeeded, or an error code if the update failed.
- **Gen'd:** Displays whether the password update attempt was automatically initiated by PAM. This value displays TRUE if PAM initiated this password update attempt automatically, for example due to a Password Composition Policy's

Maximum Password Age or a recurring Scheduled Job. This value displays FALSE if the password update was the result of a direct user action, for example if a user manually generated a new password for a Target Account.

- **Duration:** The duration of the password update attempt.
- **User:** The user that initiates the password update attempt. For example, such a user might be a PAM admin who updates a target account from the user interface, a scheduled job to update target account passwords, or the user could be the expired password processor.

### ***Account Requests***

This report lists A2A account password retrieval requests. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Target Alias Name:** The name of the target alias. (Filterable)
- **Execution User ID:** The ID of the execution user. (Filterable)
- **Request Server Host Name:** The name of the request server host. (Filterable)
- **Request Server IP Address:** The IP address of the request server. (Filterable)
- **Account Access Type:** The type of account access. (Filterable)
- **Script Name:** The name of the script.
- **Execution:** The user who executed this request.
- **Error code:** The error code generated, if any.
- **Error Description:** A description of the error code.

### ***Accounts***

This report lists target accounts. This report returns the following information:

- **Account Type:** Synchronized or Unsynchronized. (Filterable)
- **Password State:** Expired or Not Expired (Filterable)
- **Account:** Displays the target account name
- **Target Application:** The name of the target application.
- **Target Server:** Displays the target server.
- **Password Composition Policy:** Displays the Password Composition Policy.
- **Password Created:** Displays the date and time the password was created.
- **Max Pwd Age:** Displays the maximum password age, in days.
- **Password Expiry:** Displays the date and time the password expires.
- **Synchronized:** Displays whether the account is synchronized (true) or not (false).

### ***Accounts with Expired Passwords***

This report lists accounts with expired passwords. This report returns the following information:

- **Account:** Displays the account name
- **Target Application:** The name of the target application. If "unknown", the account referenced application information that was not found. Contact Technical Support for assistance with resolving this issue.
- **Target Server:** Displays the target server.
- **Password Composition Policy:** Displays the Password Composition Policy.
- **Password Created:** Displays the date and time the password was created.
- **Max Pwd Age:** Displays the maximum password age, in days.
- **Password Expiry:** Displays the date and time the password expires.
- **Synchronized:** Displays whether the account is synchronized (true) or not (false).

#### **NOTE**

You cannot filter any parameters for this report.

### ***Accounts with Incorrect Passwords***



This report lists accounts whose passwords have not verified. This report returns the following information:

- **Target Server:** The name of the target server.
- **Target Application:** The name of the target application. If "unknown", the account referenced application information that was not found. Contact Technical Support for assistance with resolving this issue.
- **Target Account:** The name of the target account.
- **Last Used:** The date and time the account was last used.

#### NOTE

You cannot filter any parameters for this report.

### **Administrative Activities**

This report lists administrative activities. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **User:** The user initiating the activity, such as a PAM administrator user name.
- **Activity:** List of administrative activity, such as Add, Update, or Delete.
- **Type:** The type of object that is involved in the activity, such as Target Server, Account, or User.
- **User Name:** Name of the object that is involved, such as Server IP address, account name, or user name. (Filterable)
- **Details:** Clarifying details, such as, for example, "Synchronized=true, Device Name=WinServer, Owner User ID=1"
- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update.
- **User Name:** The name of the user.
- **Activity:** The administrative activities, including Add, Update, or Delete. (Filterable)
- **Type of Object:** The type of object, including All, A2A Authorization, A2A Request Script or Application, A2A Request Server Default, A2A Request Server, Account History, Password Composition Policy, Password View Policy, Role, Scheduled Job, Server Key, SSH Certificate Policy, SSH Key Pair Policy, System Property, Target Account, Target Alias, Target Application, Target Server, Target or Request Group, User (Group), or User. (Filterable)

### **Authorization Mappings**

This report lists all authorization mappings. This report returns the following information:

- **Alias/(Group):** The target alias/group, such as AWS API Proxy Access Accounts,
- **Target Server:** Displays the target server.
- **Application:** The name of the target application.
- **Account:** The name of the account.
- **Request Server (Group)** The request server and its group, such as AWS API Proxy Clients.
- **Script:** The script used in the mapping.

#### NOTE

You cannot filter any parameters for this report.

### **Automatically Updated Expired Passwords**

This report lists target accounts that are updated to comply with applicable Maximum Age policy. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Pass:** Displays whether the password update was successful.
- **Account** The corresponding expired account.
- **Target Application:** The name of the target application. If "unknown", the account referenced application information that was not found. Contact Technical Support for assistance with resolving this issue.
- **Target Server:** Displays the target server
- **Password Composition Policy:** Displays the Password Composition Policy.
- **Password Updated:** Displays whether the password is updated.

- **Max Password Age:** Displays the maximum password age, in days.
- **Password Expiry:** Displays the date and time the password expires.

### **Cluster State**

This report lists cluster state changes. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Hostname:** The name of the cluster host.
- **Activity:** Lists cluster activity, such as "application cluster started".
- **Members:** The members of the cluster.
- **Origin Host Name:** The name of the origin host. (Filterable)

### **Event Processing Status**

This report lists event status for A2A request servers. This report returns the following information:

- **ID:** The identification of the event, expressed as an integer.
- **Host:** The name of the host
- **Delete:** true or false
- **Type:** Displays the type, such as master or client.
- **Status:** Display the status, where 1 is successful.
- **Site:** Displays the site, such as Primary, or the Site ID integer.
- **Oldest:** Displays the oldest event.
- **Newest:** Displays the newest event.
- **Last:** Displays the most recent event
- **New:** Displays the number of new events.
- **Success:** Displays the number of successful events.
- **Failed** Displays the number of failed events.

#### **NOTE**

You cannot filter any parameters for this report.

### **Failed Password Updates**

Lists failed attempts to change an account password. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Target Account Name:** The name of the target account. (Filterable)
- **Changes By:** The User who initiated the password update attempt. (Filterable)
- **Target Server Host Name:** The name of the target server host. (Filterable)
- **Target Application Name:** The name of the target application. (Filterable)
- **Account Access Type:** The type of account access. (Filterable)
- **Password View Policy ID:** Use the magnifying glass to filter by Password View Policy. (Filterable)
- **Error Code:** The error code generated, if any.
- **Duration:** The duration of the password update attempt.
- **Gen'd:** Displays whether the password update attempt was automatically initiated by PAM. This value displays TRUE if PAM initiated this password update attempt automatically, for example due to a Password Composition Policy's Maximum Password Age or a recurring Scheduled Job. This value displays FALSE if the password update was the result of a direct user action, for example if a user manually generated a new password for a Target Account.

### **List all Target Accounts in a Target Group**

Lists all target accounts in the target group specified in the **Target Group Name** field. This report returns the following information:

- **Hostname:** The hostname of the target account.
- **Application:** The name of the target application.
- **Account Name:** The name of the account.

#### **List all Target Applications in a Target Group**

Lists all target applications in the target group specified in the **Target Group Name** field. This report returns the following information:

- **Hostname:** The hostname of the target application.
- **Application Name:** The name of the target application.
- **Application Type:** The type of target application.

#### **List all Target Servers in a Target Group**

Lists all target servers in the target group specified in the **Target Group Name** field. This report returns the following information:

- **Hostname:** The hostname of the target server.
- **IP Address:** The IP address of the target server.
- **Device Name:** The device name of the target server.

#### **Orphaned Request Servers**

Lists all A2A request servers with no activity for one year. This report returns the following information:

- **Request Server:** The name of the request server
- **IP Address:** The IP address of the request server
- **Active:** Indicates whether the request server is active (true) or not active (false).
- **Client Type:** The type of client.
- **OS:** The operating system of the request server.
- **Date Registered:** The date of registration.

##### **NOTE**

You cannot filter any parameters for this report.

#### **Privileged Accounts**

This report lists privileged accounts. This report returns the following information:

- **Server Hostname:** Displays the server hostname or IP address.
- **Application:** The name of the target application.
- **Account:** Displays the account.
- **Access Type:** Displays the access type.
- **Date Registered:** Displays the date the registration.

##### **NOTE**

You cannot filter any parameters for this report.

#### **Requests for Invalid Aliases**

This report lists requests for aliases.

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Request Server:** The name of the request server
- **Alias:** The name of the invalid alias.
- **Script Name:** The name of the script.
- **Execution:** The user who executed this request

### ***Scheduled Jobs***

This report lists scheduled job results. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update.
- **Job Name:** The name of the job.
- **Successful:** Whether the job was successful (true) or not successful (false).
- **Command** Displays the command involved, such as scheduleReport
- **Repeats** Displays the job count.
- **Error Message:** Displays the error message, if any, such as "PAM-CMN-0680: E-mail server/account has not been set."

### ***View Password Requests***

This report lists view account password requests from the admin UI. This report returns the following information:

- **Date:** Select a **Quick Date** (such as This Month) or **Start** and **End Date** of the update. (Filterable)
- **Hostname:** Displays the hostname for the password request.
- **Application:** The name of the target application.
- **Account:** The account making the password requesting the password.
- **Reason:** Generally displays the reason for the password view entered by the requesting user, if they are required to supply one (because the **Reason Required for View** option is set in the password view policy). When integrated with a service desk solution (for example, ServiceNow), shows a predefined reason for the password view request provided by the service desk solution.
- **Workflow** (Returns Retrospective Approval, if selected.)
- **Details:** Generally displays an additional description of the reason for a password view (optionally supplied by the requesting user if they are required to supply a reason for the password view), "Not Required", or "Password Viewed". When integrated with a service desk solution, it shows details about why the target account is required.
- **Code:** Generally displays the reason code for a password view (optionally supplied by the requesting user if they are required to supply a reason for the password view). When integrated with a service desk solution, it shows the service desk ticket number.
- **Requestor:** User who executed this request.

## **Credential Manager Roles and Privileges for Running Reports**

You require a Credential Manager role with sufficient privileges to run Credential Manager Reports. The preconfigured Credential Manager ViewReports role has the following default privileges:

- Event Processing Status
- Generate Report
- List Reports
- Schedule Report

A user with the preconfigured ViewReports role can run the following set of Credential Manager reports:

- Accounts
- Accounts with Expired Passwords
- Accounts with Incorrect Passwords
- Authorization Mappings
- Automatically Updated Expired Passwords
- Event Processing Status
- Orphaned Request Servers
- Privileged Accounts
- Request for Invalid Aliases
- Scheduled Jobs
- View Password Requests

To run the other reports, a user requires a role with the default ViewReports privileges *and* the following permissions, as applicable:

Report Name	Required Additional Privileges
Account Passwords Update Attempts	<ul style="list-style-type: none"> <li>• Search Target Account</li> <li>• Search Target Server</li> <li>• Search Target Application</li> <li>• Search Password View Policy</li> </ul>
Account Requests	<ul style="list-style-type: none"> <li>• List Target Aliases</li> <li>• List A2A Clients</li> </ul>
Administrative Activities	<ul style="list-style-type: none"> <li>• Search Role</li> </ul>
Cluster State	<ul style="list-style-type: none"> <li>• Search Target Server</li> </ul>
Failed Passwords Updates	<ul style="list-style-type: none"> <li>• Search Target Account</li> <li>• Search Target Server</li> <li>• Search Target Application</li> <li>• Search Password View Policy</li> </ul>
List all target accounts in a target group	<ul style="list-style-type: none"> <li>• List Target Groups</li> </ul>
List all target applications in a target group	<ul style="list-style-type: none"> <li>• List Target Groups</li> </ul>
List all target servers in a target group	<ul style="list-style-type: none"> <li>• List Target Groups</li> </ul>

To configure a role with additional privileges, create a role (or roles) with the default ViewReports privileges *and* the new privileges. For details on how to add a new role, see [Add or Modify Credential Manager Roles](#).

For example, the following screenshot shows a new custom "ViewAllReports" role that has privileges to run all reports.

### Add Credential Manager Role

Name: \*

Description:

Available Privileges

<input type="checkbox"/> Name
<input type="checkbox"/> Reconcile Discovered Accounts
<input type="checkbox"/> Rename User
<input type="checkbox"/> Reset Client Cache
<input type="checkbox"/> Reset DB Hash
<input type="checkbox"/> Reset Group Cache
<input type="checkbox"/> Search A2A Client
<input type="checkbox"/> Search A2A Script
<input type="checkbox"/> Search Agent
<input type="checkbox"/> Search Audit Log
<input type="checkbox"/> Search Authorization
<input type="checkbox"/> Search Filter
<input type="checkbox"/> Search Group
<input type="checkbox"/> Search Password Policy
<input type="checkbox"/> Search Password View Request
<input type="checkbox"/> Search Password View Request By Approver

Selected Privileges

<input checked="" type="checkbox"/> Name
<input checked="" type="checkbox"/> Event Processing Status
<input checked="" type="checkbox"/> Generate Report
<input checked="" type="checkbox"/> List Reports
<input checked="" type="checkbox"/> List A2A Clients
<input checked="" type="checkbox"/> List Target Aliases
<input checked="" type="checkbox"/> List Target Groups
<input checked="" type="checkbox"/> Schedule Report
<input checked="" type="checkbox"/> Search Password View Policy
<input checked="" type="checkbox"/> Search Role
<input checked="" type="checkbox"/> Search Target Account
<input checked="" type="checkbox"/> Search Target Application
<input checked="" type="checkbox"/> Search Target Server

OK CANCEL

**NOTE**

If you also want a user with this role to be able to view passwords on the **Access** screen, also add the following privileges:

- Get Password View Policy
- View Account Password
- Get Target Account

## Generate Credential Manager Reports

You can generate various reports on demand on the Reports page. Audit, metric, and event data can be archived through the CLI.

**NOTE**

The size of a report is governed by a Credential Manager setting. To set the size limit, see [Schedule Credential Manager Reports](#).

**NOTE**

To view Credential Manager PDF format reports in Japanese, install the Adobe Acrobat Reader DC FontPack1900820071\_XtdAlf\_Lang\_DC fontpack.

**Follow these steps:**

1. Select **Credentials, Reports, Run**.  
The Reports page appears.
2. Select the report to generate, for example, Administrative Activities, and select **Update**. For descriptions of the reports, see [Available Credential Manager Reports](#).  
The relevant Report window appears.
3. If applicable, select a Quick Date range, or enter the Start and End Dates for the report. Reports cover the period from 00:00:00 (midnight) of the start day to 23:59:59 of the end day.
4. Specify any additional parameters, including filters, that are specific for your report.
5. Select the Output Format type (HTML, CSV, or PDF).
6. Select **OK** to run the report.  
The report displays in a new browser window.

**NOTE**

Your Web browser might first ask you to allow the report to be displayed, or might notify you that pop-ups are blocked.

## Schedule Credential Manager Reports

Credential Manager allows you to schedule jobs that run the selected report and emails the output to the selected recipients. Recipients can be selected from all Credential Manager users with a valid email address.

You can schedule report jobs with the following recurrence: daily, weekly, monthly, yearly, or after an arbitrary number of days. Alternatively, you can schedule the report to occur only once at a specified time.

Scheduled reports do not support filtering.

To view the status of scheduled jobs, generate the Scheduled Jobs Report. See [Generate Credential Manager Reports](#).

**Follow these steps:**

1. Select **Credentials, Reports, Scheduled Jobs**.  
The Scheduled Report Jobs screen appears.
2. Select **ADD**.  
The Add Scheduled Report Job dialog appears.
3. Enter the **Job Name**, which is a text description for the job, up to 80 characters long.
4. In the **Recurrence** field, select the frequency. You can select **Run Once**, **Daily**, **Weekly**, **Monthly**, **Yearly**, and **Every N Days**.
5. The **Date/Time** option changes to correspond with your **Recurrence** selection:
  1. For **Run Once**, use the **Date/Time** option to select the date and time to run one instance.
  2. For **Daily**, use the **Time** option to select the time to run a daily instance. The **Repeat Only On Weekdays** option excludes a daily run on any weekend day (Saturday and Sunday).
  3. For **Weekly**, use the **Time** option to select the time and the days of the week to run the instance.
  4. For **Monthly**, you have two options:

- **Run on day <number> of the selected month(s):** Select a date (1 to 31), or **Last** for the last day of the month to run the job. You can select one or more months to run the job using the corresponding checkbox beneath this option.
  - **Run on the <number><day> of the selected month(s):** Select First, Second, Third, Fourth, or Last day to run the job. This option allows you to specify a particular day instead of a particular date. You can select one or more days and months to run the job.
5. For **Yearly**, use the **Date/Time** option to select the date and time to run the annual instance.
  6. For **Every N Days**, use the **Date/Time** option to select the start date and time, and then how long to wait before running another instance. For example, you could select a start date, and set the time to 1 AM every four days, by setting the **Time** to 01:00:00 and the **Days** to 4.
  6. On the **Report Details** tab, in the **Report Name** field, select the type of report you want to generate.
  7. Select the **Quick Dates** for the timeframe that you want the report to cover. Reports cover the period from 00:00:00 (midnight) of the start day to 23:59:59 of the end day. The Start Date and End Date fields update automatically, and are recalculated each time that the report is run.
  8. Select one of the following Output Format options:
    - **HTML** (on the current page)
    - **CSV** (export file)
    - **PDF** (generated document)
  9. Move the desired email recipients from the **Available Recipients** list to the **Selected Recipients** list. As a default, the logged-in user is saved in the Selected Recipients list.
  10. Select **OK**.

### **Limit the Size of the Report Email Attachment**

You can configure the maximum size of a report email attachment through the system property `reportAttachmentLimit`. This system property limits the maximum size of a report email attachment. When the report exceeds the configured size set through this property, the email is not sent.

You can configure an email attachment size through the `reportAttachmentLimit` system property as shown in the following example:

Windows:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty ^
propertyName=reportAttachmentLimit propertyValues=5cspmserver_admin -u admin ^
cmdName=setSystemProperty propertyName=reportAttachmentLimit propertyValues=5
```

Linux:

```
capam_command adminUserID=admin capam=mycompany.com cmdName=setSystemProperty \
propertyName=reportAttachmentLimit propertyValues=5cspmserver_admin -u admin \
cmdName=setSystemProperty propertyName=reportAttachmentLimit propertyValues=5
```

The following table shows the details of the `reportAttachmentLimit` system property:

Property Name	Value	Required	Notes	encryptValue
<code>reportAttachmentLimit</code>	Maximum size of a report email attachment (for example, 1)	N/A	Set an integer value in MB. The default value is 5 MB.	False

## **Credential Manager Activities List**

The Credential Manager Activities page provides a set of predefined metrics to monitor system activity. Administrators with appropriate permissions can change [Configure Credential Manager Settings](#) and can apply those changes globally. Global changes affect all users of the product. Individual users can configure their own Activities list [here](#).



**Follow these steps:**

1. Select **Credential, Reports, Activities**.  
The Credential Manager Activities page appears. If you have not changed them, the default items from the Settings, Credential Manager page are listed.
2. Select the **Configure** button to change the items that are listed.  
The Credential Manager Activities Settings window appears.
3. To add a new item to the Credential Manager Activities Settings list, follow these steps:
  - a. Select the Plus icon. The Item Name window appears.
  - b. Select one or more entries from the list of available activity items.
  - c. Select **OK**. The Item Name windows closes.
4. To remove an entry from the Activities list, select the **X** icon.
5. To reposition a list item, select the item and use the Up or the Down arrow.
6. To set a threshold limit that activates a warning icon in the Activities list, enter a value in the Threshold field. For example, a threshold value of 5 for Passwords Not Verified causes a warning icon to appear in the Activities List page when the number of unverified passwords reaches 5.
7. Select **OK** to save.

## Management Console

The Privileged Access Manager Management Console is a solution for administering large cluster deployments or sets of clusters.

The Management Console helps alleviate the management burden of large installations for Managed Service Providers and other distributed deployments. The Management Console performs the following functions:

- Gathering of the site endpoints into a single location for easy navigation, similar to a launch pad
- Holding and distributing patches that can then be staged onto sites
- Gathering of basic health information from sites to present a consolidated status of the health of the clusters

Three key personas can benefit from using the Management Console:

- **Management Console Auditor:** An auditor has read-only access to the console. The auditor can evaluate patch levels and cluster health, but cannot set up clusters and cannot configure patch tasks. An auditor does not have access to the Administration function of Privileged Access Manager.
- **Management Console Operator:** An operator is able to configure the console, including staging patches. An operator cannot set up Clusters, does not have access to the Administration pages, and cannot alter Service settings.
- **Management Console Administrator** has full access to configure the console, to the Administration pages, and to launch Privileged Access Manager on managed clusters. The administrator uses the Management Console to:
  - Set up a new customer cluster.
  - Determine the health of clusters.
  - Manage patches that are available from the console.
  - Stage patches onto sites in a cluster.
  - [Approve Smart Card users to allow logins](#)
  - [Configure Active Directory for user authentication](#)

### NOTE

After the **Management Console Admin** or **Global Admin** approves the Smart Card user, make sure that the appropriate Management Console Role is assigned to these new users so they can access the **Management Console** UI. See [User Roles](#) for more information about assigning roles.

## **Initial Setup and Security**

### ***Prerequisites***

- Port 443 must be open bidirectionally within each managed cluster.
- Port 443 from each managed cluster to the MC.
- Port 443 must be open from the MC to the VIP of each managed cluster.
  - If port 443 is not open to the cluster, the Console can still monitor health and distribute patches. However, the Console operator cannot launch a session to the cluster.

### **NOTE**

The Management Console, regardless of whether it is a hardware or virtual appliance, can manage both hardware and virtual appliances.

### ***Setup***

The Management Console requires a different license, and a separate appliance (or virtual instance) on which to run the Management Console. If the Management Console is already licensed, your login defaults to the Management Console interface. If you are in the normal Administration interface, you see a Management Console link to the right of the Configuration menu. The Administration interface is limited, having some of the Configuration options, but missing most of the Provisioning settings. A Management Console appliance cannot be used as a regular Privileged Access Manager appliance.

### ***Security***

The Management Console cannot manage a cluster until its integration is configured in that cluster using information from a specific Management Console. Only one "aggregator" member of a cluster has contact with the Management Console. See [Integrate with the Management Console](#) for details.

Once configured, communication is initiated by the managed cluster. ("Launching" from **Clusters, Actions, Launch PAM** simply opens the target login page in a browser. You still have to log in.)

The managed cluster does not need to enable the external REST API.

### ***Aggregated Data***

There are two types of aggregated data: Legacy Cluster information and Time Series based meters

#### **Legacy Cluster Information**

No client-specific data is collected and transmitted outside of any managed cluster or instance. The aggregator typically sends a short status message, but sends a full report when it detects changes, or when the Management Console requests one. Status information is organized in several sections, each containing one item for each cluster member:

- Cluster Structure
  - FQDN
  - IP address
  - Master node (Boolean flag)
  - Node position (internal)
  - Record type (internal)
  - Site name
  - Site type (standalone/primary/secondary)
  - Site version (PAM version)
  - Hardware ID
- Database Status

- DB cluster status
  - DB replication role
  - Hardware ID
- License Usage (counts)
  - A2A, A2A Max
  - Access, Access Max
  - AWS Proxy, AWS Proxy Max
  - Azure Proxy, Azure Proxy Max
  - NSX Proxy, NSX Proxy Max
  - Password, Password Max (Credential Management usage count)
  - Hardware ID
- Member Performance
  - Disk free space
  - Disk total space
  - DB access status
  - Site active member flag
  - Hardware ID
- Member Staging
  - Staged patches
  - Staging status
  - Version
  - Hardware ID
- Patch Deployment
  - Patch ID
  - Status

### **Time Series-Based Meters**

To better understand overall system health, sets of meters are scraped from each VM and stored into a time series-based database. Each PAM instance has the meters for its own instance. However, after configuring the Management Console for the cluster, the meters then also aggregate to the Management Console.

This interface provides a single location to visualize the cluster activity and health from all of the cluster members.

This data is then visualized in dashboards that allows users to filter the data in various ways, including over specific time windows.

Health data includes the following information:

- CPU Utilization
- Disk, Disk I/O Utilization for PAM storage and attached Session recording storage
- Network I/O Utilization

Activity data includes the following information:

- Current users actively logged in over time
- Current active access session over time
- Current License Utilization and Utilization over time
- Cluster health status

### ***Monitoring the Management Console***

The Management Console can be set up to monitor itself. See [Integrate with the Management Console](#) for information about integrating the cluster into the Management Console.

## **Patch Delivery**

### **Prerequisite**

Patch delivery works with a firewall in place, as long as the firewall is not blocking access from the cluster to the Management Console.

## **Estimate Management Console Disk Requirements**

The Management Console retains at least 31 days of data but may temporarily maintain older data for a short period. Visualizations within the Management Console display all available data.

Internally, data is purged once a month. Therefore, for planning purposes, consider that data may accumulate for up to 62 days.

For example, if data is captured from October 1 through November 30. On December 1, the October data is removed.

### **Calculate Expected Disk Requirements:**

To estimate the disk space required for the Management Console, follow these steps:

1. Determine the total number of PAM instances across all connected clusters.
2. Add 1 for the Management Console data.
3. Use the estimated data per-node, per-day: 11 MB.
4. Apply the expected maximum retention period: 62 days.

### **Example 1:**

A single cluster with three sites, each site having three nodes (nine PAM instances in total).

**Result:** (9 PAM instances + 1 Management Console) × 11 MB × 62 days = 6.4 GB of disk space

### **Example 2:**

Two clusters:

- First cluster (production) has three sites, each site having three nodes (9 PAM instances total)
- Second cluster (UAT) has two sites with two nodes each (4 PAM instances total)

**Result:** (9 PAM instances + 4 PAM instances + 1 Management Console) × 11 MB × 62 days = 8.9 GB of disk space.

### **NOTE**

#### **Next Steps:**

- [Add a Cluster to the Console](#)
- [Integrate with the Management Console](#)
- [Enable Console Services](#)
- [Upload Patches to the Console](#)
- [View the Status of Tasks](#)

## **Add a Cluster to the Console**

The Management Console Clusters page displays the status and other properties of the clusters under management by the console. To add a cluster to the console for management, a Management Console Administrator follows these steps:

1. Go to the Management Console.
2. On the Clusters page, select **Add**.
3. On the **Basic Info** tab, create a **Name** for the cluster, and an optional Description.

4. The **Active** checkbox defaults to selected. Clear this box to add the cluster without activating it in your list.
5. The Primary Contact tab is optional, to save notes for the Management Console operator.
6. On the **Onboarding Info** tab, copy the **Cluster cookie**. You need this cookie to configure the Management Console integration on the target clusters. The Cluster VIP is read-only, and is populated when the target cluster contacts the Management Console.
7. Select **OK** to save.

To activate the cluster on the console, an administrator logs in to the target cluster to [integrate it with the console](#).

An administrator can update the optional information or can delete these clusters from the list using the Update and Delete buttons on the Cluster list. The **View Dashboard** button navigates the user to the graphical dashboard showing data meters over time for the selected cluster. **View Dashboard** is not available if you are using Internet Explorer 11.

For each cluster under management, these attributes are displayed on the Clusters page:

- **Name:** The cluster is named by the console operator.
- **Active:** If the **Active** check box is selected when you add a cluster, a check mark appears in its row. If the check box is cleared, this column reads "Inactive", and the data for that cluster row ceases to update.
  - "Not Registered" appears after the cluster has been added, but has not yet been integrated, or has not been called in yet.
  - "Pending" appears after a status refresh has been requested.
- **Last Comm:** If the most recent communication is less than a minute, a check mark appears. After one minute, it displays a warning icon with the number of elapsed minutes. After 5 minutes, it displays an error icon with the number of elapsed minutes (m), hours (h), or days (d).
- **On:** If the cluster is turned on, a check mark appears. If two or more members are sending information, a "CONFLICT" message appears.
- **Online:** If all the members in a cluster are active (in the cluster), a check mark appears.
- **Synced:** If the cluster is synced, a check mark appears. An error icon appears if the cluster is out of sync.
- **Min. Disk Free:** This column displays the disk space available in a cluster member with the least free disk space in that cluster. Any patch that is staged needs to fit on all members.
- **Version:** The Privileged Access Manager version of the reporting member is shown. All members in a cluster require the same version.
- **Members:** The total number of members in all the sites in the cluster is shown.
- **Sites:** The number of sites in the cluster is shown.
- **Licenses:** A slider graphic displays, from left to right, green, yellow, or red, to show the percent of licenses used. From 0 percent to 50 percent, the indicator is green. From 50 percent to 90 percent, the indicator is yellow. At 90 percent and above, the indicator is red.
- **Actions:** Select the arrow icon to select from these actions:
  - **View Dashboard:** Navigates the user to the graphical dashboard showing data meters over time for the selected cluster. **View Dashboard** is not available if you are using Internet Explorer 11.
  - **Launch PAM:** Open a session on the cluster.
  - **Details:** Open a page with detailed information about the cluster:
    - Number of total and used licenses for each license type, such as Session Manager
    - Information about each site, including its site membership, IP address, and status
    - Aggregator identification
    - You can stage a patch from this page, using the **Stage Patch** button. See [View the Status of Tasks](#) for more information.

Selecting the Cluster Name on the Clusters page opens this same page.

- **Refresh Status:** Select this option to request a status update from the selected cluster.
- **Send email to Contact:** Open an email that is addressed to the Email of the Primary Contact that is defined for this cluster. The email address is defined on the Primary Contact tab of the Add Cluster window. You can also access it with the Update button.

**NOTE****Next Steps:**

- [Integrate with the Management Console](#)
- [Enable Console Services](#)

## Integrate with the Management Console

To integrate your Privileged Access Manager clusters with the Management Console, a Management Console Administrator configures each cluster. You enter integration settings on one member of the Primary Site of the managed cluster, and the settings are replicated to all cluster members. An election algorithm running on the managed cluster determines which member is the aggregator who uploads information to the Management Console.

To integrate your clusters with the Management Console, you need information from the Management Console to enter into each managed cluster. Follow these steps:

1. Go to the **Administration** interface on the target cluster.
2. Go to **Configuration, Management Console, Integration**.
3. Wait to enable Integration until *after* you have tested the connection and API.
4. Enter the **Console Host Name** or **IP** address of the Management Console.
5. Enter the **Port**, such as 443, for the Management Console.
6. Select **Use SSL** if you are using SSL.
7. Enter the **API Key** and **Password** from the Management Console. Get the API Key and Password from the built-in Management Console account:
  - a. On the Management Console, go to **Administration, Credentials, Manage Targets, Accounts**.
  - b. On the Target Accounts page, find the Account Name similar to *MCApiKey-x*.
  - c. Select the View eye icon in the Action column to see the password for the API Key.
  - d. Copy the Password from the Show Password window.
  - e. Return to the target cluster and paste the password into the **Password** field of the cluster Management Console Integration page.
8. Paste the **Cluster cookie** from the Management Console for this cluster into the target cluster **Cluster cookie** field. Each cluster has its own Cluster cookie. See [Add a Cluster to the Console](#) for more information.
9. Select an **Info Upload Interval**, in minutes. We recommend that you use one minute to avoid raising warnings and alarms on the Management Console.
10. Select to **Save** the settings.
11. Select **Ping** to ensure that the cluster can communicate with the Management Console.
12. Select **Test Integration API** to ensure that the API Key, Password, and Cluster Cookie are accurate, and that the cluster can connect to the Management Console. The Management Console Services have to be running on the Management Console to succeed. If the Management Console itself is clustered, clustering must be turned on to activate the REST API.
13. Select **Enable Integration** if you are ready to report data to the Management Console.
14. Select to **Save** the settings and start reporting to the Management Console.
15. Select **Test Reporting API** to ensure that this cluster member can connect to the Aggregator member of the cluster. The managed cluster has to be on for this test to succeed.

**NOTE****Next Step:**

- [Enable Console Services](#)

## Enable Console Services

### Apply the Management Console License

Before you configure Services, apply your Privileged Access Manager license for Management Console. A license file is prepared by Broadcom Support and installed with your appliance. You update the existing license by following these steps:

1. Go to **Configuration, Licensing**.
2. Select the **Install New License** tab.
3. Use **Choose File** to locate the license file on your system. The license file is of type XCDLIC.
4. Select the **Upload License File** button.  
The **Verify New License** window appears.
5. Verify that the capabilities that are listed are expected and appropriate.
6. Select **Save New License**.
7. Log out and log back in to refresh your capabilities.

For more information about licensing, see [Apply Software and Feature Licenses](#).

### Configure Management Console Services

To configure Management Console Services, follow these steps:

1. Select the **Administration** link on the console menu.
2. Go to **Configuration, Management Console, Services**.
3. Select **Enable Services** to activate the Management Console Services, including patch distribution, and internal tasks.
4. The remaining options govern the delivery of patches to the clusters:
  - **Task Check Interval** sets the number of seconds between internal maintenance tasks. Do not change this setting unless directed by Broadcom Support.
  - **Enable Downloads** is the default mode. Clear this check box to stop distribution of any patches to any cluster.
  - **Max Number of Connections** limits the number of simultaneous connections while sending patches.
  - **Max Number of Retries** defines the number of unsuccessful attempts to download a patch before deeming it a failure.
  - **Enable Download Throttling** to keep downloading from affecting the console performance, and possibly saturating the network with Management Console traffic.
  - **Allowed Bandwidth** is in effect only if Download Throttling is selected. This setting limits cumulative bandwidth that is consumed by simultaneous patch downloads.
5. Select **Save** to save your settings.

## Upload Patches to the Console

The Management Console enables you to manage the upgrading of remote clusters and instances of Privileged Access Manager. On the Patches page, you upload patches and upgrades to the Management Console for later distribution to your managed clusters for staging.

To upload a patch, locate the Privileged Access Manager patch (for example, on the CA website) and download it to your local computer. Follow these steps to upload the patch:

1. On the **Patches** page, select the **Add** button.
2. Select **Choose File** to browse to the file, and select **Upload** to upload it. The **Archive** is the patch name.  
When a patch is uploaded to the Management Console inventory, its checksum is validated.
3. Metadata is read from the uploaded archive, and its display is read-only. These properties appear once a patch is uploaded:

- **Patch ID** identifies the patch, and can include the precise version number.
  - **Patch File** is the file name of the patch.
  - **Checksum** is presented for your validation. The hash is validated upon uploading it.
  - **Size** is specified by rounding up to the next MB.
  - **Min Level** is the lowest version number that accepts this patch.
  - **Max Level** is the highest version number that accepts this patch.
  - **Patch Type:** Upgrade or Hotfix is indicated.
  - **Reboot Type:** Member or Cluster, both, or neither are shown.
4. The optional **Information** section is intended for the Management Console operator to record how long the patch takes to execute, and any notes.
- **Duration** (in minutes)
  - **Notes**
  - **Archived:** Select the Archived checkbox to prevent the patch from being listed as a Compatible Patch in the Stage Patch Task window. Archiving allows current tasks to continue without the risks of deleting the patch, while preventing further distribution. You can return an archived patch to active duty by clearing this checkbox.
5. Click **OK** to save.

The **Update** button allows you to edit the Duration, Notes, and Archived attributes. All other Patch information is read-only. Select the row of the patch to edit, and select **Update**.

The **Patches** page lists each uploaded patch with its required information and any optional information that was provided. The following columns are displayed for each uploaded patch. This information is the same that is available during Add or Update. The Requires column combines the Min Level and Max Level fields. The Outage column displays the same information as Reboot Type.

- Patch ID
- Upload Date
- Size
- Requires
- Outage
- Duration
- Notes
- Archived

#### **NOTE**

#### **Next Step:**

- [View the Status of Tasks](#)

## Cluster Details

To see the details for an individual Cluster from the **Clusters** page, select the Cluster Name, or select **Details** from the **Actions** column.

### Cluster

The Cluster section provides cluster level details about available licenses.

### **Licenses**

License information is reported for each of the License Types that are purchased by quantity:



- Session Manager (also known as Access Devices)
- Credential Manager (also known as Password Devices)
- App to App Manager (also known as A2A Devices)
- AWS API Proxy (Users)
- NSX API Proxy (also known as VMware NSX API Proxy Users)

For each License Type, the licensed quantity is shown as Total, and the quantity being used is shown as Used. The Status graphic displays, from left to right, green, yellow, or red, to show the percent of licenses used. From 0 percent to 50 percent, the indicator is green. From 50 percent to 90 percent, the indicator is yellow. At 90 percent and above, the indicator is red.

## **Sites**

The Sites section lists each member of each site in the cluster, including the following information:

- **Site Name** displays Site Name as set in the Configuration section of that site.
- **Site Type** is either Primary or Secondary.
- **Member** displays the IP address or host name of the site (or instance).
- **Aggregator**: A check mark indicates that this member sends cluster information to the Management Console.
- **Online**: A check mark indicates that this member is online.
- **Replication**: A check mark indicates that the database is synchronized. A red exclamation mark indicates that it is not synchronized or has timed out. Mouse over the field to see the underlying status value. This field can also display "Unknown."
- **Disk Free** displays the amount of free disk space for each member. In contrast, the "Min Disk Free" column on the Clusters page shows the least amount available among all cluster members. Any patch that is staged must fit on all members.
- **Version** displays the current Privileged Access Manager version.
- **Staged** displays the patches which are staged on each member.

## **Actions**

The buttons in the Sites section allow the following actions:

**View Dashboard** Opens the *Cluster Dashboard*, an advanced visualization tool that shows current and historical system data about the selected cluster that updates over time. For more information, see [Management Console Cluster Dashboard](#).

### **NOTE**

**View Dashboard** is not available if using Microsoft Edge in Internet Explorer mode.

**Launch PAM** launches a login screen for a specific member if a site is selected, or to the cluster VIP if none is selected.

**Delete** allows you to delete a site entry from the cluster listing. The site itself is not affected and reappears at the next information upload.

The **Stage Patch** button launches the [Stage Patch Task window](#), which allows you to stage patches to the cluster. A Management Console Administrator or Operator can stage a patch.

## **Visualize Cluster Data Using the System Dashboard**

After logging into the Management Console, users see a list of configured Clusters. There are several ways to reach the visual dashboard for a particular cluster:

- Using the **Action** icon found on each of the Cluster's row, select **View Dashboard** from the menu.
- While in the Cluster details page, select the **View Dashboard** button.

Both will navigate the user to that Cluster's dashboard.

**NOTE**

When the Dashboard first loads, the Site and Instance filters will be pre-selected to include all sites and instances.

The Cluster dashboard page aggregates information from across all sites into a succinct layout, providing both current levels of key, cluster-wide data. Key data includes items such as license count and access activity, as well as changes over time.

Within the Cluster dashboard page is a table listing its PAM instances. Selecting one of those instances navigates to the PAM Single instance dashboard page. This dashboard page is the same page found on that instance of PAM.

**NOTE****Next Steps:**

- [Stage a Patch Task](#)
- [View the Status of Tasks](#)

## Stage a Patch Task

The Management Console allows you to stage tasks, such as delivering patches to your configured Privileged Access Manager clusters.

To stage a patch, follow these steps:

1. Go to the **Clusters** page.
2. Open the details for an individual Cluster by clicking the Cluster Name, or selecting **Details** from the **Actions** column.
3. The Cluster page appears, with details about available licenses, individual site members, IP addresses, and status. The Sites section of the Details page displays the current Privileged Access Manager version.
4. Select the **Stage Patch** button in the Sites section.  
The Stage Patch Task window appears, with a list of previous staging tasks, and compatible patches.  
See [Upload Patches to the Console](#) for more information about patch properties.
5. Select the appropriate Compatible Patch, and select **OK**.  
The staged patch now appears on the Tasks page.
6. To follow the status of the staged patch, you can go to the [View the Status of Tasks](#). You can reorder the rows by Cluster to help find a staged patch. The Task also appears in the Previous Staging Tasks list in the Stage Patch Task window.  
Each staged patch row displays the following information:
  - **Patch ID**
  - **Cluster** name (on the Staging Tasks page)
  - **Command** shows the most recent command, such as Recall, Retry, or Stage.
  - **Status** includes Assigned, Notified, Sending, Send Failed, Sent, Received, Dispatching, Staging, Staged, Stage Failed, Deploying, Deployed, Deploy Failed, Recalling, Recalled, and Recall Failed.
  - **Updated** shows the time that the status was last updated.
  - **Created** shows the time that the task was initiated.
  - **Attempts** displays a count of the attempts. The number of attempts is limited by the settings on the [Enable Console Services](#) configuration page.
  - **Delivered** shows the size of the patch file that is delivered.
  - **Target** cluster (only in the Stage Patch Task window)

To see details about a task in the **Previous Staging Tasks** list, select its row, and select the **Events** button. The resulting page lists each step in the staging process, with the following attributes:

- **Command** shows the type of command, such as Stage and Recall.
- **Created By** lists the User who initiated the Task.
- **Creation Time** is when the particular event was recorded.
- **Status** specifies which step in the staging flow is listed, such as Assigned, Notified, Sending, Send Failed, Sent, Received, Dispatching, Staging, Staged, Stage Failed, Deploying, Deployed, Deploy Failed, Recalling, Recalled, and Recall Failed.
- **Attempts** shows the number of attempts for the listed event.

Select **Refresh** to update the information in the Previous Staging Tasks window.

For a selected row on the Previous Staging Tasks list, you can **Retry** or **Recall** the task.

## View the Status of Tasks

To follow the status of a staged patch in the Management Console, go to the **Tasks** page. You can reorder the rows by Cluster to help find a staged patch.

Each staged patch row displays the following information:

- **Patch ID**
- **Cluster** name
- **Command** shows the most recent command, such as Recall, Retry, or Stage.
- **Status** shows the status of the task, such as Assigned, Notified, Sending, Send Failed, Sent, Received, Dispatching, Staging, Staged, Stage Failed, Deploying, Deployed, Deploy Failed, Recalling, Recalled, and Recall Failed.
- **Updated** shows the time that the status was last updated.
- **Created** shows the time that the task was initiated.
- **Attempts** displays a count of the attempts. The number of attempts is limited by the settings on the [Console Services](#) configuration page.
- **Delivered** shows the size of the patch file that is delivered.

To see details about a task in the **Staging Tasks** list, select its row, and select the **Events** button. The resulting page lists each step in the staging process, with the following attributes:

- **Command** shows the type of command, such as Stage and Recall.
- **Created By** lists the User who initiated the Task.
- **Creation Time** is when the particular event was recorded.
- **Status** specifies which step in the staging flow is listed, such as Assigned, Notified, Sending, Send Failed, Sent, Received, Dispatching, Staging, Staged, Stage Failed, Deploying, Deployed, Deploy Failed, Recalling, Recalled, and Recall Failed.
- **Attempts** shows the number of attempts for the listed event.

For a selected row on the main **Staging Tasks** page, you can **Launch PAM** on the target Cluster, and **Retry** or **Recall** the task.

## Integrating

---

The contents of this section describe how to configure the product so that it can co-operate with external, third-party devices and servers.

Use the table of contents to access the topics in this section.

### Configure Login Options for Windows Target Devices

You can configure the following options for Windows target devices:

#### Network Level Authentication Login for RDP Access

RDP sessions to a Windows server can be subject to denial-of-service (DoS) attacks. To lower the risk of DoS attacks, Windows server administrators can configure Network Level Authentication (NLA). NLA prompts a user to authenticate before a session is established with the server. PAM accommodates NLA so that connections to a Windows target server can complete successfully.

No specific configuration is required for the appliance to handle the NLA requirement. Simply add users to the Windows target device record. In the Device configuration, only the **Device Name**, **Address**, and the **Access Method** (RDP) are mandatory.

If you configure the RDP-TCP access method with the setting: **Allow connections only from computers running Remote Desktop with Network Level Authentication**, the appliance handles the NLA requirement properly. To configure the RDP-TCP access method, select the **General** tab of the **RDP-TCP Properties** dialog.

#### *User Experience with NLA*

When a user selects the RDP access method, the RDP page appears, and then a security dialog prompts for the NLA-based credentials. After the user enters the credentials, the appliance submits them to the Windows target device to complete the login operation.

#### **NOTE**

If you [enable a password push](#) for the Windows target device, this login prompt is overridden.

#### Enable a Password Push for RDP Password Enforcement

The Windows Remote Desktop Services interface has an option that is labeled **Always prompt for password**. This option allows the Windows administrator to force a password prompt even when the client workstation is configured to connect automatically.

#### **NOTE**

If NLA is enabled on an RDP server using the TLS security layer, the server ignores the **Always prompt for password** option. Users are not prompted for passwords. To enforce the password option, the Windows administrator must configure the server with the RDP security Layer.

You can configure a device group to populate the password prompt automatically, with the password obfuscated.

The following procedure assumes that you have set up the following components:

- Users
- Devices
- Target accounts
- Associated policies for auto-connection for those target accounts

**Follow these steps:**

1. Log in to the UI as an administrator with configuration privileges.
2. Navigate to **Devices, Manage Device Groups**.
3. Select an existing device group, or select **ADD** to create a group.
4. From the **Devices** tab, select the target devices that require a password push for an auto-connection policy.
5. Select the **Enable** tab, and set the **Provide Credentials for 'Always Prompt for Password'** option. This setting forces an auto-connection at the device level for any device in the device group.

**NOTE**

If the target RDP server is running 32-bit Windows 2008, you can set the **Handle 'Legal Notice' on Logon Screen** option to automatically accept the Windows legal notice that appears during login. On every other Windows version, the user must manually accept the legal notice.

6. Navigate to **Policies, Manage Policies**.
7. Prepare a policy for the user/user group and the device group that you previously configured. Select RDP as the access method for the policy.
8. Select **OK**.

**NOTE**

Windows generally presents a legal notice that the user must manually dismiss within a specified timeout period to start the session.

Password push is now enabled.

***User Experience with Password Push Configured***

When a user logs in using the RDP access method, the following actions occur:

1. The RDP Access Method splash page appears.
2. The RDP window displays the Windows login screen.
3. The appliance immediately overrides the login prompt. A brief delay occurs, during which the user sees a countdown screen until auto-connection is complete.

**NOTE**

If presented with a Windows legal notice, the user must manually dismiss that notice to start the session. If the legal notice is not dismissed within a timeout period that is defined on the server, the login session fails.

The remote user is logged in.

## Configure Kerberos PIV/CAC Authentication for Windows Targets

As an administrator, you can implement Kerberos authentication with PIV/CAC smart cards to log in to LDAP-imported Windows target devices. For Kerberos authentication, you configure connections to one or more Kerberos Key Distribution Center (KDC) servers. You then associate each applicable device group or device with a KDC.

This topic describes prerequisites for using Kerberos PIV/CAC, configuring connections to Kerberos KDC servers, associating a device group or device with a Kerberos KDC server, and logging in to a Windows target device with a smart card.

**Prerequisites for Using Kerberos PIV/CAC**

Verify the following prerequisites:

- The applicable client workstations have the approved PIV/CAC hardware and software. Up to two smart card readers can be used on each workstation.
- Network Level Authentication (NLA) is enabled on the applicable Windows RDP target devices. For more information about NLA, see [Configure Windows Target Device Options](#).
- One or more Kerberos KDC servers are available

## **Configure Connections to Kerberos KDC Servers**

Configure connections to one or more KDC servers.

### **Follow these steps:**

1. Navigate to **Configuration, 3rd Party, KDC**.
2. Select **Add** to add a KDC Server.  
The Add KDC Server Configuration window appears.
3. Enter the Kerberos KDC Server IP address and Port (typically 88).
4. Select **OK**.
5. Repeat these steps to add other KDC servers.

## **Associate a Device Group or Device with a Kerberos KDC Server**

Associate a device group or device with a Kerberos KDC server.

### **Follow these steps:**

1. Navigate to **Devices, Manage Devices**, or **Manage Device Groups**.
2. Select **Add** or **Update** to create or edit a Device or Group.
3. On the **KDC Server** tab, select the KDC Server from the drop-down list.
4. Select **OK** to save your changes.

### **NOTE**

If you specify a Kerberos KDC server at the device level, that device-level setting overrides any KDC server configuration for a device group. If a device does not have a KDC Server that is specified, only then is the KDC server for the device group used.

## **Log in to a Windows Target Device with a Smart Card**

If you are a PIV/CAC smart card user, you can log in to a destination Windows system automatically.

### **Follow these steps:**

1. Log in to the UI.
2. Select **Access** from the menu bar.
3. On the Access page, select the RDP link for the desired device to launch a connection.
4. Select **Smart Card**.
5. Complete the following steps:
  - a. Select a credential from the **Choose a smart card credential (Kerberos authentication)** drop-down list.
  - b. If your environment supports mapping one smart card certificate to multiple accounts, select **Add Hint** and enter a **Username Hint** in the field that appears.
  - c. Enter your smart card **PIN**.
6. Select **Login** to access the target Windows device.

### **NOTE**

If Kerberos is not being used, select **Login Form** to access the device.

7. (Optional) To identify the authentication protocol, select the lock icon in the top toolbar of the RDP window. A pop-up window confirms that the identity of the remote computer was verified using Kerberos.

If your credentials are correct, you are logged in to the target device.

## Kerberos Authentication Support in RDP Proxy Service

This content provides information about Kerberos functionality.

**To configure Kerberos support in RDP Proxy service, follow these steps:**

1. Navigate to **Configuration, RDP Proxy**.
2. Select **Add** to add a Kerberos Realm and KDC servers to that realm. The **Add RDP Proxy Kerberos Configuration** window appears.
3. Add the Kerberos Realm Name.
4. Enter the KDC server (IP address/FQDN) with an optional port number.
5. Select **OK**.

**Note:** You can add only one realm. Multiple Kerberos realms are not currently supported.

**Prerequisites:** The target device must be a fully qualified domain name. Defining a device with an IP address does not work for Kerberos authentication. Please ensure that PAM is able to successfully resolve all FQDNs. Also, ensure that PAM is able to ping remote desktop servers and KDC servers using their FQDNs. If using the PAM agent, ensure that the client machine, (the machine on which PAM agent is installed), is able to resolve FQDNs for remote desktop servers.

### Credential Collector for RDP Proxy service:

If no auto-login has been configured for the RDP Proxy service, then you are prompted for the credentials to log into the remote desktop server. A credential collector is displayed. Enter the following information:

- **Username:** Example: **user01**
- **Password:** Example: **mypassword**
- **(Optional) Domain:** Example: **mydomain**. If specified, this value is only used during NTLM authentication. For Kerberos authentication, the domain value is ignored. Kerberos authentication uses the realm as the domain name

**Note:** The realm value is supplied while configuring Kerberos authentication for RDP Proxy. Once you provide all required information, click Login to log into the remote desktop server. Click Cancel to cancel the login.

Once you provide all required information, click **Login** to log into the remote desktop server.

Click **Cancel** to cancel the login.

## VMware vCenter and NSX Integration

You can configure Privileged Access Manager to coordinate with a VMware installation to import virtual machines into Privileged Access Manager and apply the VMware security settings.

The Privileged Access Manager coordination with an NSX installation engages the following objects. See [Configuration tasks](#) for detailed instructions.

### VMware Requirements

Verify that you have installed NSX 6.2 or later and that it is available to Privileged Access Manager on the network.

### Privileged Access Manager Requirements

#### **Restrictions**

When VMware NSX coordination is activated in Privileged Access Manager, the following cluster synchronization features are **not** supported:



- Clustering over a WAN
- Hybrid clusters, using two or more of the three form types for Privileged Access Manager (hardware, AWS AMI instance, and VMware VMs)
- The [Access Restrictor](#) does not operate on A2A transactions.

### **Prerequisites**

- Configuration of VMware objects in Privileged Access Manager:
  - **Device:** a target vCenter
    - a Target Application for this Device
    - a Target Account for this Target Application that is an administrator account
  - **Device:** the affiliated NSX Manager
    - a Target Application for this Device
    - a Target Account for this Target Application that is an administrator account
- Configuration in of parent vCenter (**Config uration, Add VMware vCenter**)
- Configuration and activation of NSX administrator access ( **Configuration, VMware NSX**)

Following configuration and registration, the NSX and Privileged Access Manager effects include:

*In Privileged Access Manager:*

- **Device imports** – vCenter virtual machines are imported (a Device record is created for each VM)
- **Security controls** – Existing NSX Security Tag, Security Group, and Security Policy restrictions are imposed on vCenter devices that are imported into Privileged Access Manager.

*In NSX:*

- **Privileged Access Manager Service** – A new NSX partner service named "Privileged Access Manager Service" is created, with Profile Configurations for these functions:
  - **Session Recording**
  - **Terminate Sessions**
  - **Privileged Access Manager Re-Authentication**
- **Dynamic effects** – As NSX Security Tag, Security Group, and Security Policy definitions are altered over time, the effects are propagated from NSX to Privileged Access Manager.
- **Access restrictor** – Privileged Access Manager dynamically pushes its access policies for mirroring as NSX distributed firewall exceptions. Thus these rules are created as connections open, and are destroyed when those connections close.

### **Coordination with NSX**

When you configure Privileged Access Manager to coordinate with an NSX installation, Privileged Access Manager begins sharing objects that are managed in NSX. Following registration, you can (manually) specify controls on VMs by applying VMware Security Tags to VMs directly. You can use the NSX Service Composer to define Security Groups and impose Security Policies on those groups, which affect imported Privileged Access Manager devices. This process applies two features that are illustrated here:

- Service Composer integration with Privileged Access Manager Service
- Dynamic transfer of NSX Security Groups and Security Tag assignment to Privileged Access Manager

### **Access Restrictor**

When Privileged Access Manager is registered in NSX, and before it connects to a managed VM, it pushes its access policy for that connection into NSX as a distributed firewall *exception*. It instructs NSX to temporarily "poke a hole" through the firewall managing the VM to allow the Privileged Access Manager-authorized connection.

### **Permitted Connections Tracked**



You can impose a highly restrictive but distributed NSX firewall without concern about it interfering with Privileged Access Manager-managed access to targets. NSX auditing is aided in this manner, because now the logging and recording capabilities of Privileged Access Manager are explicitly imposed on any connections making it through the otherwise broadly imposed firewall.

### ***Verifiable in NSX Manager***

In the NSX Manager **Firewall** panel, you see the Access Restrictor rule being applied for the active connection. This rule automatically occupies highest precedence order over other rules and thus is applicable to the connection. When the Privileged Access Manager-managed connection is closed, this exception rule is deactivated and removed.

### **NSX Service Composer Security Controls**

Three pre-defined NSX Service Profile Configuration controls are provided in the product Service that is registered when you configure the product to work with a vCenter and an NSX installation that is associated with that vCenter.

Any of those Profile Configurations can be specified in an NSX Security Policy. That policy is applied to an NSX Security Group of VMs. The members of that Security Group might consist of, for example, those VMs with certain Security Tags or labels, such as "Surveillance\_Target", that can be applied at any time deemed necessary by the administrator.

### ***Dynamic Event Infrastructure***

The following NSX callbacks that are built in to the Privileged Access Manager Service are created in NSX when a Privileged Access Manager registers to an NSX installation. When any of the following Service Profiles have been activated in NSX Security Policy applied to Devices imported from VMware, Privileged Access Manager imposes the described actions to the active Privileged Access Manager connection sessions:

- **Terminate Sessions** – Prevent any future session attempt from consummating.
  - User receives a pop-up message during a current session or session attempt.
  - Terminate Sessions works for all connection types. Event is logged and is captured in session recordings.
- **Session Recording** – Switch session recording on or off.
  - NSX policy overrides Privileged Access Manager Policy setting.
  - Works for RDP, SSH, and Telnet Access Method applets; RDP Applications; all native SSH or Telnet Services; CA PAM Browser (HTTP and HTTPS)
  - Event is logged and is captured in session recordings.
- **Privileged Access Manager Re-Authentication** – One-time (non-recurring) application to force Users to re-authenticate to Privileged Access Manager.
  - User receives an interactive pop-up message to submit credentials.

### ***Provisioning in Following NSX Tagging***

Privileged Access Manager imports the Security Tags and Security Groups of VMs into Device records to manage the connection to these VMs. Basic device characteristics (name, address, OS, VMware directory) populate the Device records. Unassigned, user-defined Security Groups and Security Tags are always imported because you can provision policies before tags are assigned. For example, if the policies to be used are complex.

Changes in the NSX environment are propagated each time a Privileged Access Manager User loads their Access page. Changes to NSX Security objects are dynamically applied in Privileged Access Manager. NSX Manager executes callbacks to the product whenever its Security Groups or Security Tags are updated. The product can make the corresponding adjustments and can propagate any policy effects.

### **NOTE**

Assign the same name to a Security Group and associated Security Tag when the Security Group contains only items with a single Security Tag.

These imported tags can then be assigned to Device Groups to impose the desired controls.

When Security Groups or Security Tags are created in an NSX installation running a Privileged Access Manager Service, or they are newly assigned to NSX devices, these changes propagate to Privileged Access Manager in several ways:

- When a tag (either local, or VMware-imported Security Group or Security Tag) is assigned to a Device Group, the Devices that the tag specifies are identified as members of the Device Group.
- If you apply an unused tag to a Device Group and you use that group in an active Privileged Access Manager policy, and then later assign the tag to a device in NSX, the corresponding Privileged Access Manager Device and corresponding policy is dynamically activated. The policy becomes available on the User Access page.

You can prepare compact Privileged Access Manager policies that are also complex and powerful.

## **Configuration Tasks**

Perform the following tasks to activate coordination of an NSX installation with your Privileged Access Manager.

### ***Preparation***

You must have the following applied:

- VMware vCenter applicable with NSX 6.2.
- Privileged Access Manager licensing applied: **VMware Capability**

### **Register Privileged Access Manager in NSX Manager**

VMware configuration has been expanded to allow use of multiple vCenter deployments, and now (for a single vCenter) allows synchronization of an NSX deployment. The VMware configuration panel set on the **Configuration, 3rd Party** page has been expanded with a new **VMware** page.

### ***Prerequisites***

- Registration with NSX requires that a single vCenter is configured in Privileged Access Manager. Multiple vCenter configurations, although permitted, cannot be used while there is an active NSX registration.

### ***Procedure***

To provision preliminary Devices and Accounts, and configure vCenter and NSX, follow these steps:

1. Prepare VMware target Device records:
  - a. In Privileged Access Manager, navigate to **Devices, Manage Devices**.
  - b. Add a Device record for vCenter with **Address=Your-vCenter-portal-address**
  - c. Add a Device record for NSX with **Address=Your-NSX-Manager-portal-address**
2. Prepare corresponding target accounts to access:
  - a. Navigate to **Credentials, Manage Targets, Applications**:
    - a. **Add** a new target application for vCenter.
    - b. **Add** a new target application for NSX.
  - b. Navigate to **Credentials, Manage Targets, Accounts**:
    - a. **Add** a new target account for the vCenter target application you created.
    - b. **Add** a new target account for the NSX Manager target application you created.
3. Navigate to the **Configuration, 3rd Party, VMware** page.
4. **Add** a previously **Configured VMware vCenter**:
  - a. In the **vCenter Authentication Device** field, select from the drop-down list the vCenter Device you prepared earlier.
  - b. In the **vCenter User** field, select from the drop-down list the vCenter access target account you prepared earlier.
  - c. In the **URL** field, enter the URL address of the vCenter. Include the port and any subdirectory path.
  - d. Select **Device Sync** to attempt to import from this account immediately following an **Add**. Syncs then continue according to the Global VMware vCenter Sync period.
  - e. Click **OK**.

5. On the **VMware NSX** tab:
  - a. In the **NSX Authentication Device** field, select from the drop-down list the NSX Manager Device you prepared earlier.  
In the **NSX User** field, select from the drop-down list the NSX access target account you prepared earlier.
  - b. In the **URL** field, enter the URL address of the NSX installation. Include the port and any subdirectory path.
6. On the **Refresh Interval** tab:
  - a. Select a Refresh Interval from the drop-down list. The interval begins on the next multiple according to the system clock. For example, "5 Minutes" causes a sync to start at the next multiple of 5 minutes, such as 12:25.
  - b. Select **Update**.
  - c. You can force all vCenter Account combinations to import newly active provisions at the next fixed refresh interval.  
On the **Configured VMware vCenter** tab, select **Global VMware Sync**.

### **Confirm Registration**

You can confirm that NSX has created "Xsuite Service" by inspecting the Networking & Security Service Definitions in a vSphere client.

## **Additional Privileged Access Manager Registration Options**

### **Re-register NSX Manager**

When your NSX Manager registration fails, the VMware NSX fields remain, but Status changes from "Not Configured" to "Not Registered".

- After you correct the issue, you can again attempt registration using the staged settings by clicking **Save**.
- Otherwise, you can remove all settings by clicking **Disable**.

### **Unregister NSX Manager**

To unregister Privileged Access Manager in NSX:

1. Take care to back out of all corresponding settings you had applied in Privileged Access Manager and NSX.
2. When that is completed, select **Unregister** in the **VMware NSX** panel.
3. The currently registered Privileged Access Manager Service is removed from NSX, and the NSX Manager is unregistered in Privileged Access Manager.

### **Options for Updates**

- **Access page runtime updates**  
NSX synchronization with Privileged Access Manager is initiated whenever the Access page is loaded. **Note:** This feature increases Access page load time.
- **Background updates**  
Privileged Access Manager updates are initiated after NSX settings are updated, and after each vCenter Refresh Interval.

#### **NOTE**

- [NSX Provisioning Examples](#)

## **NSX Provisioning Examples**

You can configure Privileged Access Manager to coordinate with a VMware installation to import virtual machines into Privileged Access Manager and apply the VMware security settings. We include two examples of NSX provisioning to assist with your VMware integration.

### Example 1: Preparation of an NSX Security Policy for Privileged Access Manager Use

You can impose any of the above three controls on Devices managed by Privileged Access Manager from within NSX features. The following procedure shows how this process works by completing the following steps:

- Creating Security Policies that specify access controls
- Creating Security Groups that dynamically specify a set of devices
- Applying those policies to those groups to activate their controls on their devices. These controls are propagated to Privileged Access Manager, and then imposed when Users access VMware-imported Devices.

Following registration of Privileged Access Manager with NSX, open your vSphere Client or Web Client:

1. From the vSphere home, select the **Networking & Security** item from the left menu.
2. From the new left menu items, select the **Service Composer** item, and then in the Service Composer body select the **Security Policies** tab to display the (currently empty) policies list.
3. Above the item list in the far left, select the Create Security Policy icon to open a policy editing window.
4. Specify a policy that imposes Privileged Access Manager session recording, and call it "Session Recording SP":
  - a. Select the **1 Name and description** tab, and enter in the **Name** field "Session Recording SP".
  - b. In **2 Guest Introspection Services**, select the icon further right to open an editing window. In it:
    - a. For **Service Name**, select "Privileged Access Manager Service"
    - b. For **Service Profile**, Select "Session Recording (Data Collection)"
    - c. Leave the other fields and buttons as is, and select **OK**.
 The editing window now disappears, and you see the new service specification as a line item.
  - c. In **4 Network Introspection Services**, perform the same previous steps for (b), except that here you edit the **Profile** field rather than the **Service Profile**.
  - d. In the lower right corner, select the **Finish** button to activate the Security Policy.

With procedures parallel to the preceding procedures for the other two Service Profiles, you can prepare corresponding policies. The following table lists the three Service Profile options currently made available through Privileged Access Manager Service registration.

#### Privileged Access Manager Service: Service Profiles

Privileged Access Manager Service: Service Profiles	Description
Session Recording (Data Collection, Vulnerability Management)	Toggles the Privileged Access Manager-based session recording policy: Where Privileged Access Manager policy for a connection has recording off, NSX turns it on, and vice versa.
Terminate Sessions (Vulnerability Management, Data Collection)	Terminates current connection sessions and prevents new sessions from being initiated.
Privileged Access Manager Re-Authentication (Data Collection, Vulnerability Management)	Suspends current Privileged Access Manager User login sessions and forces the Users to reauthenticate. Where reauthentication succeeds, the login session resumes and the previous session state is restored. Where re authentication fails, the login session is terminated.

After preparing Security Policies for all three Service Profiles, you will see three Security Policies listed.

## Example 2: Dynamic Application of an NSX Security Policy for Privileged Access Manager Session Recording

With an NSX Security Policy in place to switch Privileged Access Manager session recording, you can prepare an example of that Service Profile in action:

1. From the same location in your vCenter client as you used when preparing Security Policies ([Example 1](#)), select the **Security Groups** tab to open its pane.  
(The list might be empty except for Activity Monitoring Data Collection.)
2. To record all current and future connection sessions to certain devices, create a Security Group named "Capture Sessions SG":
  - a. Select the **1 Name and description** tab, and enter in the **Name** field "Capture Sessions SG".
  - b. In **2 Define dynamic membership**, and in the pane at the right named **Membership criteria 1**:
    - a. In the lower left drop-down list, select "Security Tag" to specify that the VMs with a Security Tag are included in this group.
    - b. In the lower center drop-down list, select "Equals to".
    - c. In the field to the lower right, enter "Capture Sessions ST".
  - c. In the lower right corner, select the **Finish** button to activate the Security Group, as we have provided the definition that we need for this group.
3. Apply the Security Policy that you created earlier to this Security Group:
  - a. Select again the Security Policies tab to open its pane.
  - b. Select the Rank number for the **Session Recording SP** policy so that the line item is selected, then right click and select **Apply Policy** from the pop-up menu.
  - c. Select the **Capture Sessions SG** group and select **OK**.
4. Apply a Security Tag to a VM device. This illustrates how the Security Group picks up the tagged device for imposition of the policy, and the effect of that policy for Privileged Access Manager.
5. Navigate from the vSphere home:
  - a. Select the **vCenter** item from the left menu.
  - b. From the new left menu items, select the **Hosts and Clusters** item.
  - c. In the left panel (with left tab at top selected), open the tree until you find an (existing) VM to which you would like to apply this Security Group. In this example, the device is named "BEE".
6. The VM device ("BEE") has a number of specification panels. Apply the tag that is specified when you created the "Capture Sessions SG" Security Group. That is, "Capture Sessions ST":
7. Select the "BEE" line item. Then in the device specification section to the right, in the **Security Tags** pane:
  - a. Select the **Manage** link in the lower right corner of the pane.
  - b. In the **Assign Security tag** pop-up window, select the icon to create the new "Capture Sessions ST" tag.
  - c. When created, scroll to the location of the new tag, and select it.
  - d. Select **OK** to close the pop-up.  
The "Capture Sessions ST" tag is listed in the **Security Tags** pane. The "Capture Sessions SG" that uses that tag is also specified in the **Security Groups** pane.  
Because that group has the "Capture Sessions SP" Security Policy applied against it, then when a Privileged Access Manager User attempts a connection session to BEE – whether the Privileged Access Manager policy itself specifies session recording – Privileged Access Manager activates recording.
8. Navigate Privileged Access Manager to the **Devices, Manage Devices** page.
  - a. Open the Device record for "BEE".  
**Note:** You can also continue instead with a Privileged Access Manager-based Device Group that includes this Device. In place of a fixed, imported tag, manually apply the imported Security Tag as described in the following steps.

There is an editable "Privileged Access Manager-assigned-tag-3". There are also two tags which are not editable in Privileged Access Manager: "NSX-SG-Capture Sessions SG" and "NSX-TAG-Capture Sessions ST".

These reflect the Security Group and Security Tag that were imported from VMware.

9. Navigate to the **Policies, Manage Policies** page.
  - a. Create (or open) a policy for BEE (and you, the current administrator User).  
Do *not* assign a recording policy.
10. Navigate to the **Access** page, and open a connection session to BEE.
11. Navigate to the **Sessions, Session Recordings** page.  
You see near the top of the line items that a session recording has begun to BEE.  
The VMware Security Policy overruled the (empty) Privileged Access Manager recording policy, dynamically imposing session recording.

## VMware NSX API Proxy Integration

### WARNING

**Warning:** VMware NSX API support is deprecated and will be removed in a subsequent version of PAM.

VMware NSX API Proxy requires licensing from CA Technologies for a specific number of proxy users. The proxy is available for deployment in VMware OVA file format.

### NOTE

If your Privileged Access Manager installation allows use of both VMware NSX API Proxy and AWS API Proxy, these proxies must be on different subnets.

The use case flow is:

1. A user sends a REST API request (intended for NSX Manager) to the new CA Technologies VMware NSX API Proxy. The request uses credentials from Privileged Access Manager, which are valid only for use with this proxy. (They differ from the credentials that are used by NSX Manager).
2. The proxy validates the request, obtains the actual (and persistent) NSX Manager credentials that have been vaulted on Privileged Access Manager. The proxy then uses those credentials to forward the request to NSX Manager.
3. The NSX Manager response is passed directly to the user. Audit and request syslog entries are stored in vCenter Log Insight. If configured, Privileged Access Manager rotates the NSX Manager credential.

A VMware NSX API Proxy User role has the accessAll and manageAll privileges, and a **VmwareNsxApiProxy** role allows use of the proxy.

### Auto-Activation Whitelist

Only NSX API Proxies which are within specified subnets are permitted to receive NSX Manager credentials automatically from Privileged Access Manager. Such subnets are called "whitelisted subnets." Specify these whitelists as follows:

1. Navigate to the **Configuration, 3rd Party, VMware NSX API Proxy** page.
2. In the **NSX API Proxy Auto-Activation Whitelist** tab, select **Add**.  
The **Add NSX Subnet** window appears.
3. Enter a private subnet that contains the NSX API Proxy instances. Use CIDR form (for example, 10.21.1.0/24), and select **OK**.  
You receive a green confirmation message at the top of the page: "NSX API Proxy Auto-Activation Whitelist successfully updated."



# Managing Java on Your Client Workstation

This content describes how to manage Java on your client workstation.

## Clear the Java Cache (Windows)

To help prevent mismatched Java cache contents during or after upgrading a Windows client workstation, clear the Oracle Java cache.

To clear the Java cache, open the Java control panel (**Control Panel, Java**) and remove all "Temporary Files".

## Update the Java Heap Setting

We recommend that you adjust your Java heap so that with 4 GB of total memory, 1024 MB is allocated to it. An example of the adjustment mechanism would be to Assign the Java maximum heap size value in **Runtime Parameters**:

```
-Xmx1024m -Xms1024m
```

### **NOTE**

Do not copy-and-paste the string into a word processor (such as Microsoft Word) before pasting into the Java Control Panel. This action might alter the characters. Instead, if you want to store the string, use a plain-text application such as Notepad.

To confirm that the heap adjustment has taken effect: When your mouse is in focus in the Java console, press: m to display the memory values. If successful, the results are close to the settings.

## Applet JAR File Signing

By default, Privileged Access Manager JARs are signed and are validated against a public Certificate Authority (CA). For many customers, this arrangement is sufficient and no further action is required. However, if your users do not have access to the public Internet, this feature provides an alternative.

If you are considering self-signing, we suggest you discuss this strategy first with Broadcom Support.

## **Certificate Configuration**

You can sign JAR files using certificates that are issued from any CA, including one located in an isolated internal network. Use this procedure to set the signing certificate.

### **To use a certificate from a CA, follow these steps:**

1. Have your organization CA administrator prepare a code-signing certificate.  
You receive the public certificate and private key for signing the JARs. You also receive the public key of the CA that issues this certificate with its CRL.
2. Log in as Privileged Access Manager User "config", or as another account with at least a role of Configuration Manager. For example, you can also use "super".
3. Navigate to **Configuration, Security, Certificates**.
4. On the **Upload** tab, **Browse** to your certificate files and **Upload** them.  
Upload at least the public certificate and private key, and these files must have the same root name. The public and private key files should end with the ".crt" and ".key" extensions respectively; for example, you might have "ExampleCorp1.crt" and "ExampleCorp1.key".
5. On the **Sign Applets** tab, enter the node IP address as the **Domain**. For a cluster, use the primary VIP.
6. Select the **Certificate** with the bundle root name you uploaded, or the Default Applet Certificate.
7. To confirm the certificate integrity, select **Verify**, and note the confirmation message at the top of the page.

8. After the certificate passes verification, select **Sign Applets**. Wait a few moments for the Privileged Access Manager applets to be signed, and confirmed at the top of the page.
9. Clear your Java cache.
10. Log out from Privileged Access Manager, and then log back in.

**To use the Default Applet Certificate, follow these steps:**

1. On the **Sign Applets** tab, enter the appliance IP address as the **Domain**. For a cluster, use the primary VIP.
2. Select Default Applet Certificate as the **Certificate**.
3. To confirm the certificate integrity, select **Verify**, and note the confirmation message at the top of the page.
4. After the certificate passes verification, select **Sign Applets**. Wait a few moments for the Privileged Access Manager applets to be signed and confirmed at the top of the page.  
To ensure that you access the signed JAR files, follow these steps:
5. Clear your Java cache.
6. Log out from Privileged Access Manager, and then log back in.

### **Client Configuration**

To configure a client to trust the certificate that is used to sign the applet JARs, add the certificate to one of the following locations:

#### **Your Java JRE installation**

To add the certificate to your client Java installation, follow these steps:

1. Open the Java Control Panel.
  - In Windows, open `c:\Program Files\Java\jreX.X.X_X\bin\javacpl.exe`.
  - On a Mac, select System Preferences, Java, Java Control Panel.
2. In the Java Control Panel, select the **Security** tab, and the **Manage Certificates** button.
3. Select the **Certificate Type** "Signer CA".
4. On the **User** tab, select the certificate, and select **Import**.
5. Browse to the location of the certificate and select **Open**.
6. Select **Close** and **OK**.

#### **Your browser certificate store**

To add the certificate to Internet Explorer, follow these steps:

1. Select the **Tools** icon or the Tools menu, then select **Internet Options**.
2. Select the **Content** tab, then select the **Certificates** button.
3. In the Certificates windows, select the **Import** button.
4. Select **Next**, then the **Browse** button to locate the certificate file. Select **Open**.
5. Select **Next**, then "Automatically select the certificate store based on the type of certificate."
6. Select **Next**, then inspect the settings summary. If you approve, select **Finish**.  
A status message appears.

## **Juniper Integration**

You can allow use of manual login to access a Privileged Access Manager appliance behind a Juniper Networks SSL VPN, rather than configuring Privileged Access Manager auto-connection access.

### **User experience**

While logged in to Juniper, open the login page through a Juniper bookmark, and manually log in.



## Juniper setup

1. Log in to Juniper.
2. Set up a bookmark to the Privileged Access Manager login page:  
For the **URL** string for that bookmark, append the following tag:

?XSUITE\_VPN\_LOGIN=1

**Example:** `https://xsuite.example.com/?XSUITE_VPN_LOGIN=1`

### NOTE

Remember to add a trailing slash "/" to the Privileged Access Manager address/path.

## User experience (after configuration)

1. Log in to Juniper.
2. Select the Juniper bookmark you created earlier, and open the Privileged Access Manager login page.
3. Log in to Privileged Access Manager.

# Integrate a Java Application or Application Server

The following method has been tested with a WebLogic version 12.2.1 application server.

## Setup

To modify a Java application or application server (such as Weblogic, JBoss, or Tomcat) into a requestor, modify them to use the Privileged Access Manager JARs and native code libraries:

- The JAR files must be in the class path of the requestor. The JAR files are `cspmclient.jar` and `cwjcafips.jar`. They are located in the `$CSPM_CLIENT_HOME/cspmclient/lib` directory.
- If the requestor uses the Privileged Access Manager JDBC proxy, the `cloakwareJdbc.jar` file must be in the class path of the requestor. It is located in the `$CSPM_CLIENT_HOME/cspmclient/tools` directory.
- The library path of the requestor must include `$CSPM_CLIENT_HOME/cspmclient/lib`.

Setting the class path can be done in the standard Java manner or might be application-specific. The latter is a common requirement of application servers. See your application documentation for details.

The library path can be set:

- As part of the requestor Java invocation using the `-Djava.library.path` syntax
- Using the OS-specific environment variable. The possible environment variables are `PATH` for Windows, `LD_LIBRARY_PATH` for Solaris and Linux, and `LIBPATH` for AIX.

## Using the Privileged Access Manager JDBC Proxy Driver

The Privileged Access Manager JDBC driver is a proxy for the original Database Management System (DBMS) JDBC driver. Without A2A, the requestor has a JDBC connection to a DBMS. The requestor is configured with the following information:

- The class of the JDBC driver, which must be in the class path of the requestor
- Information about where it is connecting (the DBMS' hostname, and so on)
- Extra driver parameters, such as the username and password to log in as, the driver buffer sizes, and so on.

To use Privileged Access Manager JDBC driver:

1. Change the driver reference from the original DBMS-specific one to the Privileged Access Manager JDBC driver. The driver class name becomes `com.ca.pam.a2a.client.jdbc.JdbcDriver`.

2. Change the JDBC connection string to add information specifying the Privileged Access Manager JDBC driver name, the target alias that identifies the target account, and the class name of the original DBMS JDBC driver as follows:
3. 1. Prefix the JDBC connection string with `capam`.
2. Suffix the JDBC connection string with `;CSPMDriver=targetDriverClassName;CSPMAlias=alias` where:
  - `targetDriverClassName` is the class name of the original DBMS JDBC driver (such as `oracle.jdbc.driver.OracleDriver` for Oracle, `com.microsoft.sqlserver.jdbc.SQLServerDriver` for Microsoft SQL Server, `com.mysql.jdbc.Driver` for MySQL, `org.postgresql.Driver` for Postgres, or `com.ibm.db2.jcc.DB2Driver` for DB2)
  - `alias` is the target alias that is associated with the target account the requestor uses to log in to the DBMS

CA Technologies also recommends that the username and password fields be cleared out. They are overwritten by the Privileged Access Manager JDBC proxy driver.

The following example shows a modified connection string to an Oracle database:

- **Before:** `jdbc:oracle:thin:@//dbHost:1521/myService`
- **After:** `capam:jdbc:oracle:thin:@//dbHost:1521/myService;CSPMDriver=oracle.jdbc.OracleDriver;CSPMAlias=myAlias`

## Integrate with Your Service Desk Solution

As a system administrator, you can configure Privileged Access Manager to provision privileged account access to your service desk solution.

### Password View and Update

Administrators create password view policies for target service desk accounts. The policy can dictate the interaction between a user password request and the application. When a user asks to view a privileged account password, the service desk application prompts for a service desk ticket number. The application uses the ticket number to validate the user.

The following IT service management products have password update or view capabilities:

- BMC Remedy version 8.1 and 9.1
- CA Service Desk Manager r14.1 and r17.0
- HP Service Manager version 9.32 and 9.41
- ServiceNow Jakarta and Istanbul
- Salesforce Service Cloud Winter 2015 release (supports password viewing, but not updating)

### Auto-Connect to an Application

To log in automatically to the service desk application, configure a password view policy to the privileged user account. This policy can use a service desk ticket number to connect automatically to the application.

### Service Desk Logs

If you have to troubleshoot your service desk integration, you can download CA NIM logs. Use this option only with the aid of Broadcom Support. For more information, see [Configure Diagnostic Logs](#).

### Integration Instructions for Your Service Desk Solutions

To obtain specific integration procedures for your service desk application, select the corresponding entry from the table of contents.

## CA NIM UM and SM Integrations

CA Normalized Integration Management User Management (CA NIM UM) and Service Management (CA NIM SM) let PAM integrate with various third-party service desk solutions. These solutions provide a normalized generic API to create Incidents in service desk products.

The product includes the following CA NIM pre-existing components:

- Device (Target Server) – displayed on the Manage Devices page, cannot be edited.
- Two target applications – one for User Management (CA NIM UM), one for Service Management (CA NIM SM)
- Two accounts – one for each application type. Both accounts are named **nimadmin**.

The only configuration task for CA NIM accounts is to change the default passwords for the two nimadmin accounts. The default password is nimadmin.

### Follow these steps to change the default passwords:

1. Log in to the UI and select **Credentials, Manage Targets, Accounts**.
2. Select the checkbox for one of the nimadmin accounts and select **Update**.
3. Enter a new password in the Password field.
4. Select **OK**.
5. Repeat the procedure for the other nimadmin account.

## Clarity Service Desk Manager Integration

As a system administrator, you can configure Privileged Access Manager to provision privileged account access to Clarity Service Desk Manager (formerly CA Service Desk Manager).

### Prerequisites

Before you configure the settings for Clarity Service Desk Manager, verify that you have an appropriate version. To enable password updates by Privileged Access Manager, ensure that Clarity Service Desk Manager is configured for PIN-based authentication.

### **Supported Versions**

- Clarity Service Desk Manager r14.1 and r17.0
- Clarity Service Desk Manager REST Services are installed and deployed. REST Services are not deployed by default. To deploy them, use the following command:

```
pdm_rest_util -deploy
```

For more information, see your Clarity Service Desk Manager documentation.

### ***PIN-Based Authentication***

Clarity Service Desk Manager contact records do not have a "password" field, but another field is used for the password. A Clarity Service Desk Manager administrator can specify a contact record field such as contact\_num or email\_address to be used for passwords. Therefore, updating a password through Privileged Access Manager updates that same field.

### **To enable PIN-based authentication, follow these steps:**

1. On the Clarity Service Desk Manager system, navigate to Administration, Security and Role Management, Access Types.
2. Select the Access Type for which you are enabling PIN-based authentication.
3. On the Web Authentication tab, select PIN from the Validation Type drop-down list.
4. Select Save.

For more information, see the following topics in the Clarity Service Manager documentation at [techdocs.broadcom.com](http://techdocs.broadcom.com):

- Configuring User Accounts
- Create an Access Type
- User Authentication

### **Device Configuration**

To integrate with Clarity Service Desk Manager, create a target server device.

#### **Follow these steps:**

1. Navigate to **Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Enter the **Name** and **Address**.
3. Enter a description. The description displays on the Devices panel as Description.
4. Select the **Operating System**.
5. Select the **Device Type**.
6. The remaining values are optional, and are described in [Device Setup](#).
7. Select **OK**.

### **Application Configuration**

Next, set up an Application for Clarity Service Desk Manager.

#### **Follow these steps:**

1. Go to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.  
The Add Target Application window appears.
3. Select the Select magnifying glass icon to select the SDM device you created.
4. The **Host Name** and **Device Name** are populated.
5. Enter "SDM" or similar into the **Application Name** field.
6. Select "SDM" from the **Application Type** drop-down list.  
A details box is added to the Application Details panel. Each ITSM solution has its own detail fields.
7. Select a Password Composition Policy if you have created one.
8. Add Descriptor 1 and 2, optionally.
9. Enter the SOAP Protocol, SOAP Port, REST Protocol, and REST Port.
10. Enter the `DefaultAttachmentRepositoryName`.
11. Enter the PIN Field (such as `contact_num` or `email_address`) that Clarity Service Desk Manager is using as password.
12. Select **OK**.

### **Account Configuration**

Set up the Account using the Device and Application you have already set up.

1. Go to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.  
The Add Target Account window appears.
3. Select the Find Server magnifying glass icon to select the SDM device you created.  
The **Host Name** and **Device Name** are populated.
4. Select the Select magnifying glass icon to select the SDM application you created.  
The SDM Account Details box is added to the Account window, with the Change Process selection.
5. Enter a name into the **Account Name** field.
6. Leave the Password View Policy as Default unless you already have one to use.

7. Enter a password or select the Generate Password icon. Generating a password disables the Show Password check box.  
**Note:** The remaining password-related fields are read-only. The maximum age and expiration fields are determined by the Password Composition Policy, if any. See [Construct Password Composition Policies](#) for more information.
8. Select a Synchronized option. The default is to change only the Password Authority Server. To change the password on the target server also, select "Update both."
9. In the SDM Account Details box, select the Change Process. Select whether the Account can change its own password, or can indicate another account. If the user does not have permission to change passwords, use another account. Selecting "Use the following account to change password" displays a list of existing accounts.
10. You can optionally select an Owner User Name from the list of users on the CA Privileged Account Manager system.
11. Select **OK**.  
 The Message "The account was saved successfully" appears.

### **Password View Policy Configuration**

Each target account is associated with a password view policy, either the default policy or a policy that you create. See [Establish Password View Policies](#) for more information. Using Service Desk Integration in a Password View Policy requires the user to enter a service desk ticket number.

#### **Follow these steps:**

1. Go to **Credentials, Workflow, Password View Policies**.
2. Select the Add button. The Add Password View Policy window appears.
3. On the **Service Desk** tab, select CA Service Desk Manager from the **Service Desk Integration** drop-down list. Specific SDM configuration fields appear.
4. Enter the **SDM Server** name, the **SDM Application** name, and the **Account** name.
5. You can be more specific in your ticket number request: limit the type of ticket, or use a query filter. **Ticket Type** defaults to All. Incident, Problem, and Request are also available. See [Query Filter](#) for details about Query Filters. On the **Basic Info** tab, Reason Required For View and Reason Required For Auto-Connect are checked. These options are required for service desk integration. A warning appears if you try to clear either checkbox.
6. You can use more credential workflows methods, such as dual authorization and re-authentication. See [Establish Password View Policies](#) for more information.
7. Select **OK**.  
 A message appears: "The Password View Policy Has Been Saved Successfully"

### **Query Filter**

Create Queries with the Query Filter field. Use combinations of values that are used to filter which service desk tickets are used for validation.

#### **Field Values**

- **Impact:** entireorganization, multiplegroups, none, oneperson, singlegroup, smallgroup
- **Priority:** highpriority, lowpriority, medium-highpriority, medium-lowpriority, mediumpriority, none
- **Severity:** allhandsescalation, escalated, hdmgrescalation, mgrescal, supervisorsescal
- **Status:** acknowledged, analysiscomplete, approvalinprogress, approved, avoided, awaitingenduserresponse, awaitingvendor, cancelled, closed, closedunresolved, closerequested, fixed, fixinprogress, hold, inprogress, knownerror, open, pendingchange, problem-closed, problem-fixed, problem-open, rejected, researching, resolved, sa-abandon, sa-resolved
- **Urgency:** immediate, quickly, soon, veryquickly, whenpossible

#### **Operators**

```

== (equals)
&& (and)
|| (or)
!= (not equals)

```

### Examples

```

status==acknowledged
status!=closed
status==open
(urgency==immediate&&priority==highpriority)||status==inprogress&&impact==none

```

## HP Service Manager Integration

Complete the following tasks to enable the appliance to work with HP Service Manager:

### Prerequisites

Before you configure the settings for HP Service Manager, ensure that HP Service Manager uses GMT as the time zone. If not, when you use the timestamp to search for users, the search fails. See your HP Service Manager documentation for more information.

To consume Service Manager tables, fields, and display actions, you must grant an operator the SOAP API or RESTful API capability word.

### Follow these steps in the HP Service Manager UI:

1. From the System Navigator, select **System Administration, Ongoing Maintenance, Operators**.
2. Enter or select your search criteria, and then select **Search**.
3. Select an operator from the record list to view the operator record.
4. Select the **Startup** tab.
5. Add `RESTful API` or `SOAP API` in the Execute Capabilities section.

### HP Service Manager Configuration

Configure the operator WSDL file from the HP Service Manager UI.

### Follow these steps:

1. Select **Tailoring, Web Services, Web Service Configuration**.
2. Enter the Name as **Operator**, select search, and select the **Operator** from the **Object Name**.
3. Select the **Fields** tab to enable **ContactName**, select the **contact.name** from the **Field list**, and give the **ContactName** against the **contact.name**, and select **Save**.
4. To delete, go to the **Allowed Actions** tab, select **Delete** from the **Allowed Action list**, and select **Save**.
5. To get **userName** in **Get users by filter** response:
  - a. Enter the Name as **Contacts**, select **Search**, and select the **Contact** from the **Object Name**.
  - b. Select the **Fields** tab, select the **operator.id** from the **Field list** and give the **Name** against the **operator.id**, and select **Save**.

### Add a Device

To integrate with HP Service Manager, create a target server device.

**Follow these steps:**

1. Navigate to **Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Enter the **Name**, **Address**, and optionally, a description.
3. Select the **Operating System**.
4. For the **Device Type**, select all applicable options. To create a target application and account later, you must select **Password Management**.
5. The remaining values are optional, and are described in [Device Setup](#).
6. Select **OK**.

**Define a Password Composition Policy**

If you want to manage HP Service Manager passwords in the appliance, avoid certain special characters. The HP Service Manager web service that we use for integration does not accept these special characters in passwords:  `; ; ? / \ "`

Create a Password Composition Policy to configure the policy to avoid these characters.

**Follow these steps:**

1. Go to **Credentials, Manage Targets, Password Composition Policies**.
2. Select the **Add** button.  
The Add Password Composition Policy window appears.
3. Enter a **Name** and optionally, a **Description**.
4. In the **Must Not Contain** section, select **Characters To Exclude**. In the adjacent text field, enter  `; ; ? / \ "`
5. Ensure that these same characters do not appear in the text fields for **Must Contain** or **First Must Contain**. If characters exist in both "must contain" and "must not contain" conditions, the policy fails when you select **Test** or **OK**.
6. See [Construct Password Composition Policies](#) for more information about the remaining fields.
7. Select **Test** to test the policy. Select **OK** to save the policy.

**Add a Target Application**

Set up an Application for HP Service Manager.

**Follow these steps:**

1. Go to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.  
The Add Target Application window appears.
3. Select the Select magnifying glass icon to select the HP Service Manager device you created.  
The **Host Name** and **Device Name** are populated.
4. Enter "HP Service Manager" or similar into the **Application Name** field.
5. Select "HP Service Manager" from the **Application Type** drop-down list.  
An HP Service Manager Details box is added to the Application Details panel. Each ITSM solution has its own detail fields.
6. Select a **Password Composition Policy** if you have created one.
7. Add Descriptor 1 and 2, optionally.
8. On the **HP Service Manager** tab, enter the Port or accept the default of 13080.
9. Enter the **HP SM Client URL**. The initial field value suggests the correct format for the URL (`http://hpsm-host-name:port-number/webtier-9.41`).
10. Enter the **Enabled Protocol** or accept the default of `http`.
11. If HP Service Manager uses a proxy, enter the parameters as appropriate.
12. Select **OK** to save the application.



## Add a Target Account

Set up the Account using the Device and Application you have already set up.

### Follow these steps:

1. Go to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.  
The Add Target Account window appears.
3. Select the Find Server magnifying glass icon to select the HP Service Manager device you created.  
The **Host Name** and **Device Name** are populated.
4. Select the Select magnifying glass icon to select the HP Service Manager application you created.  
The HP Service Manager Account Details box is added to the Account window, with the Change Process selection.
5. Enter a name into the **Account Name** field.
6. Leave the **Password View Policy** as Default unless you already have one to use.
7. Enter a password or select the **Generate Password** icon. Generating a password disables the **Show Password** check box.
8. On the **Password** tab, select **Discovery Allowed** if you want to enable Account Discovery. See [Use Account Discovery to Add Target Accounts](#) for more information.
9. The remaining password-related fields are read-only. The maximum age and expiration fields are determined by the Password Composition Policy, if any. See [Construct Password Composition Policies](#) for more information about Password Composition Policies.
10. Select a Synchronized option. The default is to change only the Password Authority Server. To change the password on the target server also, select "Update both."
11. On the HP Service Manager tab, select the **Change Process**. Decide whether the account can change its own password. If not, select another account in the **Use the following account to change password** field. If the user does not have permission to change passwords, use another account.
12. Select **OK** to save the Account.  
The Message "Target account saved" appears.

## Establish a Password View Policy

Each target account is associated with a password view policy, either the default policy or a policy that you create. See [Establish Password View Policies](#) for more information. Using Service Desk Integration in a Password View Policy requires the user to enter a service desk ticket number.

### Follow these steps:

1. Go to **Credentials, Workflow, Password View Policies**.
2. Select the Add button. The Add Password View Policy window appears.
3. On the **Service Desk** tab, select HP Service Manager from the Service Desk Integration drop-down list.  
Specific HP Service Manager configuration fields appear.
4. Enter the **HP Service Manager Server** name, the **HP Service Manager Application** name, and the **Account** name.
5. You can be more specific in your ticket number request by limiting the type of ticket or by using a query filter. **Ticket Type** defaults to All. Incident, Problem, Change, and Request are also available. See [Query Filter](#) for details about Query Filters.
6. On the **Basic Info** tab, Reason Required For View and Reason Required For Auto-Connect are checked. These options are required for service desk integration. A warning appears if you try to clear either checkbox.
7. You can use more credential workflows methods, such as dual authorization and re-authentication. See [Establish Password View Policies](#) for more information.
8. Select **OK**.  
A message appears: "The Password View Policy Has Been Saved Successfully"



## **Specify a Query Filter for Validation**

The Query Filter field enables you to create queries that filter which service desk tickets are used for validation.

### ***Field Values***

- **Impact:** enterprise, multiple users, site/dept, user
- **Status:** accepted, closed, open, pending change, pending customer, pending other, pending vendor, referred, rejected, replaced problem, resolved, work in progress
- **Urgency:** average, critical, high, low

### ***Operators***

== (equals)

&& (and)

|| (or)

!= (not equals)

### ***Examples***

status==accepted

status!=closed

status==open

(urgency==critical&&impact==enterprise)||status==open&&urgency==high

## **BMC Remedy ITSM Integration**

To integrate with BMC Remedy service management platform, complete the prerequisites and the ITSM configuration.

### **Prerequisites**

Before you configure the settings for BMC Remedy ITSM, copy the SDK JAR files from the BMC Remedy System. These files enable communication between the appliance and the BMC Remedy Service Desk application.

### **Follow these steps:**

1. On the BMC Remedy system, go to the following directory:  
 \\bmc\Software\ARSystem\Arserver\api\lib
2. Copy the following SDK JAR files:
  - arapi\*.jar
  - arutil\*.jar
3. Save the copied JAR files to a location accessible to the appliance.
4. In the UI, select **Configuration, 3rd Party, Remedy Service Desk..**
5. On the **Upload File** tab, use the **Choose File** button to browse for the JAR files individually. Use the Upload button to upload each file, one at a time.
 

**Note:** If you are load balancing, you have to upload the JAR files to each server. The files are the same for Windows and Linux.
6. On the **Remedy Service Desk Files** tab, restart the app server by clicking the **Restart Tomcat** button. Wait until the process completes.  
 A message displays: "Tomcat restarted successfully."

## **Configure the Remedy Device**

To integrate with BMC Remedy ITSM, create a target server device.

### **Follow these steps:**

1. In the UI, navigate to **Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Enter the **Name** and **Address** of the Remedy application server. If your Remedy web server is separate from your application server, ensure that this address is for the application server.
3. Enter a description. The description displays on the Devices panel as Description.
4. Select the **Operating System**.
5. Select the **Device Type**.
6. The remaining values are optional, and are described in [Device Setup](#).
7. Select **OK**.

## **Add the Target Application and Connector**

Next, set up a target application and target connector for BMC Remedy.

### **Follow these steps:**

1. Go to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.  
The Add Target Application window appears.
3. Use the Select magnifying glass icon to select the Remedy device you created.  
The **Host Name** and **Device Name** are populated.
4. Enter "Remedy" or similar into the **Application Name** field.
5. Select Remedy from the **Application Type** drop-down list.  
The **Remedy** tab appears.
6. On the Remedy tab, enter the **Port** or accept the default of 0.
7. Enter the **Remedy Client URL**, which is for the Remedy web server. If your Remedy web server is separate from your application server, ensure that this address is for the web server. The initial field value suggests the correct format for the URL:  
`(href="http://bmc-client-host-nameport-number" scope="external">http://bmc-client-host-name:port-number/arsys )`
8. Select a **Password Composition Policy** if you have created one, or you can leave the default "None."
9. Add Descriptor 1 and 2, optionally.
10. Select **OK**.

## **Specify the Target Account**

Set up the Account using the Device and Application you have already configured.

### **Follow these steps:**

1. Go to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.  
The Add Target Account window appears.
3. Select the Find Server magnifying glass icon to select the Remedy device you created.  
The **Host Name** and **Device Name** are populated.
4. Use the Select magnifying glass icon to select the Remedy application you created.  
The Remedy Account Details box is added to the Account window, with the Change Process selection.
5. Enter a name into the **Account Name** field.
6. Leave the Password View Policy as Default unless you already have one to use.

7. Enter a password or select the Generate Password icon. Generating a password disables the Show Password check box.  
**Note:** The remaining password-related fields are read-only. The maximum age and expiration fields are determined by the Password Composition Policy, if any. See [Password Composition Policies](#) for more information about Password Composition Policies.
8. Select a Synchronized option. The default is to change only the Password Authority Server. To change the password on the target server also, select "Update both."
9. In the Remedy Account Details box, select the Change Process. Decide whether the Account can change its own password, or you can indicate another account. If the user does not have permission to change passwords, use another account. Selecting "Use the following account to change password" displays a list of existing accounts.

#### NOTE

Remedy users with the "AR User Fixed" or "AR User Floating" license type can update their own password. For other users, select "Use other account", and specify a Remedy user with a fixed or floating license.

10. Optionally, select an Owner User Name from the list of users available to the appliance.
11. Select **OK**.

### Set Up a Password View Policy (Optional)

Each target account is associated with a password view policy, either the default policy or a policy that you create. See [Establish Password View Policies](#) for more information. Using Service Desk Integration in a Password View Policy requires the user to enter a service desk ticket number.

#### Follow these steps:

1. Go to **Credentials, Workflow, Password View Policies**.
2. Select the Add button. The **Add Password View Policy** window appears.
3. On the **Service Desk** tab, select Remedy from the Service Desk Integration drop-down list. Specific Remedy configuration fields appear.
4. Enter the **Remedy Server** name, the **Remedy Application** name, and the **Account** name.
5. In the **Ticket Type** field, specify the type of ticket record for the policy. The default is All but the options Incident, Problem, Change, and Request are also available. You can also use a [query filter](#) to narrow the tickets for validation.
6. On the **Basic Info** tab, Reason Required For View and Reason Required For Auto-Connect are checked. These options are required for service desk integration. A warning appears if you try to clear either checkbox.
7. You can use more credential workflows methods, such as dual authorization and re-authentication. See [Password View Policies](#) for more information.
8. Select **OK**.  
 A message appears: "The Password View Policy Has Been Saved Successfully"

### Filter Service Desk Tickets (Optional)

To filter which service desk tickets are used for validation, use the **Query Filter** field. Create queries with combinations of the following fields and operators:

#### Fields and Values

Field Name	Values
impact	high, low, medium, minor
priority	critical, high, low, medium
status	assigned, cancelled, closed, inprogress, new, pending, resolved
urgency	critical, high, low, medium

## Operators

Operator	Meaning
==	equals
&&	and
	or
!	not equals

### Example Query Filters

- `status==active`
- `status!=closed`
- `status==open`
- `(urgency==critical&&priority==high) || status==inprogress&&impact==high`

## ServiceNow Integration

Learn how to configure the ServiceNow target connector to enable PAM to communicate with ServiceNow service management software.

Complete the procedures in this topic to integrate PAM with ServiceNow. Before you begin, contact ServiceNow and confirm that the services are accessible so that PAM can integrate with ServiceNow applications.

### NOTE

The integration with ServiceNow only supports the following ticket types: **Incident**, **Request**, and **Change**.

Complete the following tasks to integrate PAM with ServiceNow:

### Prerequisites

This section describes prerequisites for integrating with a ServiceNow server.

#### ***Required ServiceNow Roles for the Connection API Type***

PAM can connect to ServiceNow using either of its API protocols:

- SOAP web service interface
- REST API

The ServiceNow account that you configure as the target account must be assigned the roles that are required for the chosen API type.

#### **ServiceNow SOAP API Roles:**

- SOAP-related roles: `soap`, `soap_query`, `soap_script`
- Web service admin role: `web_service_admin`
- For Get Incident & Request & Change: `odbc` role
- Roles that are assigned in the ACLs of tables: `incident`, `sys_db_obj`, `sys_user`, `sys_dictionary`, `sys_journal_field` and `task` tables for read permissions. (Contact your ServiceNow admin If you need help with ACL roles).

#### **ServiceNow REST API Roles:**

- personalize\_dictionary
- u\_journal\_entry\_user
- web\_service\_admin>
- catalog\_admin
- itil & itil\_admin

### **Configuration Prerequisites If Accessing ServiceNow Via a Proxy Server**

If you are accessing ServiceNow using a proxy server, configure a device for that server. If the proxy server requires a password, also configure a target application and target account for the proxy server.

#### **Follow these steps:**

1. Navigate to **Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Complete the following fields:
  - Enter the **Name** and **Address** of the proxy server.
  - Enter a description. The description displays on the **Devices** panel as **Description**.
  - Select the **Operating System**.
  - Set the **Password Management** option under **Device Type**.
  - The remaining values are optional, and are described in [Device Setup](#).
3. Do one of the following steps:
  - If the proxy server has no password, select **OK** and proceed to [Configure an Access Device for the ServiceNow Server](#).
  - If the proxy server has a password, select the **Save and Add Target Applications** button and continue this procedure.
4. In the **Add Target Application** window that appears, complete the following fields:
  - Select the proxy device that you created.  
The **Host Name** and **Device Name** are populated.
  - Enter "ServiceNow Proxy" or similar into the **Application Name** field.
  - Select **Generic** in the **Application Type** field.
  - Leave all the other fields in their default state.
5. Select **OK**.
6. To create a target account, go to **Credentials, Manage Targets, Accounts**.
7. Select the **Add** button.  
The **Add Target Account** window appears.
8. Complete the following fields:
  - In the **Host Name** field, enter the host name or IP address of the device you created for the proxy server, or select the magnifying glass icon and select the proxy server from the list in the **Target Servers** dialog that appears.
  - Select the target **Application Name**.
  - Enter the proxy **Account Name**.
  - Leave the **Password View Policy** as Default.
  - Enter the proxy account **Password**.  
The remaining password-related fields are read-only. If you configure a password composition policy, the maximum age and expiration fields are determined by this policy. To configure a password policy, see [Password Composition Policies](#).
9. Select **OK**.

### **Configure an Access Device for the ServiceNow Server**

To integrate with ServiceNow, first create an access device.

**Follow these steps:**

1. Navigate to **Devices, Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Enter the **Name** and **Address**.
3. Enter a description. The description displays on the Devices panel as Description.
4. Select the **Operating System**.
5. Set the **Password Management** option under **Device Type**.
6. The remaining values are optional, and are described in [Device Setup](#).
7. Select **OK**.

**Configure a Target Application for the ServiceNow Server**

Configure a target application for the ServiceNow server.

**Follow these steps:**

1. Go to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.  
The **Add Target Application** window appears.
3. Complete the following fields:
  - Select the ServiceNow device that you created.  
The **Host Name** and **Device Name** are populated.
  - Enter "ServiceNow" or similar into the **Application Name** field.
  - Select **ServiceNow** in the **Application Type** field. (The **ServiceNow** tab appears.)
4. Select the **ServiceNow** tab and complete the following ServiceNow-specific configuration fields:
  - Enter the ServiceNow **URL**. The initial field value suggests the correct format for the URL (`https://servicenow-host-name/`).
  - Enter the **ServiceNow Client URL**. The initial field value suggests the correct format for the URL (`https://servicenow-host-name/`).
  - If the ServiceNow instance uses a custom endpoint, enter "true" in the **Custom Endpoint** field. If not, leave the default setting of "false."
  - Specify the type of ServiceNow API to use:
    - **SOAP** (the default)
    - **REST**
  - If ServiceNow uses a proxy server, enter the following parameters:
    - **Proxy protocol**: Specify the protocol required to access the ServiceNow proxy server (HTTP or HTTPS).
    - **Proxy server**: Specify the hostname or IP address of the ServiceNow proxy server.
    - **Proxy application**: If the proxy server requires a password, specify the target application that you configured earlier.
    - **Proxy account**: If the proxy server requires a password, specify the target account that you configured earlier.
    - **Proxy port**: Specify the port number to access ServiceNow on the proxy server.
5. Select **OK**.

**Create a Target Account for the ServiceNow Server**

Now that you have a device and target connector, specify the target account.

**Follow these steps:**

1. Navigate to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.  
The **Add Target Account** dialog appears.

3. In the **Host Name** field, enter the host name or IP address of the device you created for the ServiceNow server, or select the magnifying glass icon and select the ServiceNow server from the list in the Target Servers dialog that appears.
4. Select the ServiceNow application in the **Application Name** field.  
The **ServiceNow** tab is added to the Account window, with the Change Process selection.
5. Enter the name of the ServiceNow user account designated for PAM integration in the **Account Name** field.  
**NOTE**  
Verify that the ServiceNow account is assigned the [roles that are required for the chosen API type](#) (SOAP or REST).
6. Leave the **Password View Policy** as Default unless you already have one to use.
7. Enter a **Password** or select the **Generate Credential** icon. Generating a password disables the Show Password check box.  
The remaining password-related fields are read-only. If you configure a password composition policy, the maximum age and expiration fields are determined by this policy. To configure a password policy, see [Password Composition Policies](#).
8. On the **Password** tab, select a **Synchronized** option. The default is to **Update only the Credential Manager Server**. To also change the password on the target server, select **Update both the Credential Manager Server and the target system**.
9. Also on the **Password** tab, optionally select an **Owner User Name** from the list of users on the appliance.
10. On the **ServiceNow** tab, optionally select the **Change Process**. Decide whether the Account can change its own password, or can indicate another account. If the user does not have permission to change passwords, use another account. Selecting "Use the following account to change password" displays a list of existing accounts.
11. Select **OK** to save your changes.

### **Define a ServiceNow Password View Policy**

Each target account is associated with a password view policy, either the default policy or a policy that you create. Using Service Desk Integration in a Password View Policy requires the user to enter a service desk ticket number.

For more information about view password policies and how to use them for credential workflows, see [Password View Policies](#)

#### **Follow these steps:**

1. Go to **Credentials, Workflow, Password View Policies**.
2. Select the **Add** button. The **Add Password View Policy** window appears.
3. Enter a **Name** (for example, "ServiceNow") for the password view policy.
4. On the **Service Desk** tab, select ServiceNow from the Service Desk Integration drop-down list.  
Specific ServiceNow configuration fields appear.
5. Enter the **ServiceNow Server** name, the **ServiceNow Application** name, and the **Account** name.
6. Use the **Ticket Type** drop-down to narrow the ticket number request. The default is **All**, but the options **Incident**, **Problem**, **Change**, and **Request** are individually selectable. You can also use a [query filter](#) to narrow the scope of service desk tickets for user validation.

#### **NOTE**

Although the **Problem** appears in the **Ticket Type** drop-down, the ServiceNow integration does not support it; do not select it or use it in a query filter.

7. On the **Basic Info** tab, Reason Required For View and Reason Required For Auto-Connect are checked. These options are required for Service Desk integration.
8. Select **OK**.

## Assign the New Password View Policy to Target Accounts

Assign the new ServiceNow password view policy to target accounts of users who require a valid ServiceNow

ticket to view their password. To do this, use the search icon (🔍) beside the **Password View Policy** to select your ServiceNow password view policy when [adding or modifying a target account](#).

## Filter Service Desk Tickets (Optional)

To narrow which service desk tickets are used for validation, use the **Query Filter** field. Create queries with combinations of the following fields and operators:

### Fields and Values

Field Name	Values
impact	high, medium, low
priority	critical, high, moderate, low, planning
status	Ticket type: <ul style="list-style-type: none"> <li>Incident: new, active, awaiting problem, awaiting user info, awaiting evidence, resolved, closed</li> <li>Change: pending, open, work in progress, closed complete, closed incomplete, closed skipped</li> <li>Request: pending approval, approved, closed complete, closed incomplete, closed cancelled, closed rejected</li> </ul>
urgency	high, medium, low

### Operators

Operator	Meaning
==	equals
&&	and
	or
!	not equals

### Example Query Filters

- `status==new`
- `status!=closed`
- `status==awaiting problem`
- `status==active|| (status==awaiting problem)`

## Salesforce Service Cloud Integration

### Device Configuration

To integrate with Salesforce Service Cloud, create a target server device.

#### Follow these steps:

1. Navigate to **Manage Devices** under the **Devices** menu. Select the **Add** button.
2. Enter the **Name** and **Address**.
3. Enter a description. The description displays on the Devices panel as Description.



4. Select the **Operating System**.
5. Select the **Device Type**.
6. The remaining values are optional, and are described in [Device Setup](#).
7. Click **OK**.

### **Application Configuration**

Next, set up an Application for Salesforce Service Cloud.

#### **Follow these steps:**

1. Go to **Credentials, Manage Targets, Applications**.
2. Select the **Add** button.  
The Add Target Application window appears.
3. Click the Select magnifying glass icon to select the Salesforce Service Cloud device you created.  
The **Host Name** and **Device Name** are populated.
4. Enter "Salesforce Service Cloud" or similar into the **Application Name** field.
5. Select "Generic" from the **Application Type** drop-down list.
6. Select a Password Composition Policy if you have created one, or leave the default "None."
7. Add Descriptor 1 and 2, optionally.
8. Click **OK**.

### **Account Configuration**

Set up the Account using the Device and Application you have already set up.

#### **Follow these steps:**

1. Go to **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button.  
The Add Target Account window appears.
3. Click the Find Server magnifying glass icon to select the Salesforce Service Cloud device you created.  
The **Host Name** and **Device Name** are populated.
4. Click the Select magnifying glass icon to select the Salesforce Service Cloud application you created.  
The Salesforce Service Cloud Account Details box is added to the Account window, with the Change Process selection.
5. Enter a name into the **Account Name** field.
6. Leave the Password View Policy as Default unless you already have one to use.
7. Enter a password or click the Generate Password icon. Generating a password disables the Show Password check box.  
**Note:** The remaining password-related fields are read-only. The maximum age and expiration fields are determined by the Password Composition Policy, if any. See [Password Composition Policies](#) for more information about Password Composition Policies.
8. You can optionally select an Owner User Name from the list of users on the CA Privileged Account Manager system.
9. Click **OK**.  
The Message "The account was saved successfully" appears.

### **Password View Policy Configuration**

Each target account is associated with a password view policy, either the default policy or a policy that you create. See [Password View Policies](#) for more information. Using Service Desk Integration in a Password View Policy requires the user to enter a service desk ticket number.

**Follow these steps:**

1. Go to **Credentials, Workflow, Password View Policies**.
2. Select the Add button. The Add Password View Policy window appears.
3. On the **Service Desk** tab, select Salesforce Service Cloud from the Service Desk Integration drop-down list. Specific Salesforce Service Cloud configuration fields appear.
4. Enter the **SFDC Server** name, the **SFDC Application** name, and the **SFDC Account** name.
5. Enter the **SFDC Login Endpoint** URL. The initial field value suggests the correct format for the URL ( `https://login.salesforce.com/services/Soap/u/32.0f` ).
6. Enter the **SFDC Service Cloud Client** URL. The initial field value suggests the correct format for the URL ( `https://sfdc-instance-name` ).
7. Enter the **Date Format** of Salesforce Service Cloud. The default is `yyyy-MM-dd'T'HH:mm:ss.SSS'Z'` .
8. Enter **Case Object**, **Case Comment Object**, and **Attachment Object** according to your Salesforce Service Cloud configuration.
9. See [Query Filter](#) for details about Query Filters.
10. If SFDC uses a proxy, enter the parameters as appropriate on the **SFDC Proxy** tab.
11. On the **Basic Info** tab, Reason Required For View and Reason Required For Auto-Connect are checked. These options are required for service desk integration. A warning appears if you try to clear either checkbox.
12. You can use more credential workflows methods, such as dual authorization. See [Password View Policies](#) for more information.
13. Click **OK**.  
A message appears: "The Password View Policy Has Been Saved Successfully"

**Query Filter**

The Query Filter enables you to create Queries with combinations of values to filter which service desk cases are used for validation.

***Field Values***

- **Status:** new, escalated, on hold, waiting on customer, working, researching, closed
- **Priority:** critical, high, medium, low

***Operators***

`==` (equals)

`&&` (and)

`||` (or)

`!=` (not equals)

***Examples***

```
status==new
```

```
status!=closed
```

```
(status==new&&priority==critical)||status==working&& priority=high
```

## Privileged Access Manager Server Control Login Integration

As a security administrator, you want to audit the actual user of your server, not the shared local privileged user name. Privileged Access Manager Server Control Login Integration allows Privileged Access Manager to integrate the login process and information with Server Control. When activated, it allows the use of the actual user name for auditing in Privileged Access Manager Server Control.

## Configure Server Control Login Settings

Integration of Server Control Login requires configuration of specific Server Control settings and the creation of the following endpoint definitions:

- Device
- Account
- Application
- Policy

### NOTE

To use server names instead of IP addresses, verify that DNS Servers are configured in the Network Configuration section. From the UI main page, select **Configuration, Network, Network Settings**. Verify that in the **DNS Servers** field, a DNS IP address is listed. If none is listed, add your DNS Servers. Select Update to save the changes.

## Enable Legacy Server Control Configuration

Set up ActiveMQ for Server Control on the Server Control. Some information from the Server Control setup is required.

1. Log in to the PAM UI.
2. Select **Configuration, Server Control**.
3. Set the **Enable Legacy Login Integration** option.
4. Enter the target server hostname or IP address in the **ENTM Host Name or IP** field.
5. Enter the **Port** number, or accept the default 61616.
6. Enter the **ActiveMQ Broker Account**. The default is "reportserver."
7. Enter the ActiveMQ Broker Account **Password** and **Confirm** it.
8. Optionally, specify a different **Message time-to-live** value (the default is 60 minutes).
9. Optionally, specify a different **Reply Timeout** (the default is 10 seconds).
10. Optionally, disable TLS (the default is enable).
11. Select **Ping AMQ Console** when complete.
12. Verify that your information is correct and select **Save**.

## Create a Device

Create a Device for the Privileged Access Manager Server Control endpoint.

1. Select **Devices, Manage Devices**.
2. Select **Add** to create a device.
3. Enter the host name in the **Name** field.
4. Enter the IP address in the **Address** field. To verify the IP address, select **Scan**.
5. Specify the target **Operating System**.

### IMPORTANT

Always specify the applicable operating system. Use of the "Other" setting causes access failure when a PAM user attempts to log into the specified device.

6. Set the **Password Management** option.
7. Select the **Access Methods** tab and select the plus sign (+) button to add an Access Method.
8. Select the access type (such as SSH or RDP) from the **Name** drop-down list.  
Specific access method details appear. Add or alter the information as necessary.
9. All other fields on all tabs are optional.
10. Select **OK** to save your changes.

## Create an Application

Create an Application for the Privileged Access Manager Server Control endpoint.

1. Select **Credentials, Manage Targets, Applications**.
2. Select the **Add** button to create an application.
3. Enter the host name in the **Host Name** field or use the magnifying glass icon to the right to select from existing Devices.
4. Enter the **Device Name**. (Selecting an existing device using the magnifying glass icon to the right of the **Host Name** field also populates this field.)
5. Enter the target **Application Name**.
6. Select the **Application Type**.

#### IMPORTANT

Do not select the "Generic" option; doing so can result in access issues.

Certain Application Types display more options when selected. For example, Windows Proxy allows selection of Local or Domain Account. Most fields are optional or show a default value.

7. Select **OK** to save your changes.

#### NOTE

Windows or Windows proxy applications using a local account require that you use the target device's machine name (netbois name) in the **Name** field of the target device.

### Create an Account

Create an Account for the Privileged Access Manager Server Control endpoint.

1. Select **Credentials, Manage Targets, Accounts**.
2. Select the **Add** button to create an account.
3. Enter the host name in the **Host Name** field or use the Select magnifying glass icon to the right to select from existing Devices.
4. Enter the **Device Name**. (Selecting an existing device using the Select magnifying glass icon to the right of the **Host Name** field also populates this field.)
5. Use the magnifying glass icon to the right of the **Application Name** field to select from Applications that have already been created for the Device. Alternatively, use the Add Target Application plus sign (+) icon to add an application directly from this screen.
6. Enter the **Account Name** to use for connecting to the Server Control endpoint.
7. Enter the **Password** for the Account Name that you selected.
8. Other fields are optional. At this point, you may want to enable password management options. For more information, see [Protect Privileged Account Credentials](#).
9. Select **OK** to save your changes.

### Create a Policy

Create an Access Policy for the Server Control endpoint.

1. Select **Policies, Manage Policies**.
2. Select the **Add** button to create a policy.
3. Select the **User** to use for connecting to the Server Control device.
4. Select the Server Control **Device**.
5. On the **Access** tab, select one or more entries from the **Available Access** list and move them to the **Selected Access** list.
6. On the **CA PAM Server Control** tab, set the **Login Integration** option.
7. Other fields are optional.
8. Select **OK** to save your changes.

### Test the Login Integration

To test Privileged Access Manager Server Control Login Integration, connect through the Access link on the Access Management page. Verify the user name substitution.

1. Select **Access**  
A list of Device Names appears with corresponding Access Methods and Target Applications.
2. Select the Access Method link (such as RDP or SSH) for the Server Control Device you are integrating.  
An RDP or SSH session opens to the Device.
3. For Windows RDP, open PowerShell or the Command prompt. For Linux, use the SSH prompt.  
The prompt includes the local Server Control privileged user login, not the Privileged Access Manager user.
4. For Windows, enter "secons -whoami". For Linux, enter "/opt/CA/AccessControl/bin/sewhoami -a".  
Server Control secons utility writes several lines of text.
5. Find the "PUPM User". This should be the Privileged Access Manager user, not the local Server Control privileged user.

## Symantec SiteMinder Integration

As a security administrator, you can integrate Privileged Access Manager with Layer7 SiteMinder (formerly CA Single Sign-On). You can use Layer7 SiteMinder as a second layer of protection for Privileged Access Manager. First you authenticate to Privileged Access Manager, then to Layer7 SiteMinder, which is also auditing access to Privileged Access Manager.

### NOTE

Privileged Access Manager does not support integration with Layer7 SiteMinder for AWS instances in this version.

### Prerequisites

- Layer7 SiteMinder Policy Server requires manual set-up before setting up Privileged Access Manager. Depending on your environment, you configure many of the following objects on the Policy Server:  
Agent, Agent Configuration Object, Host Configuration Object, Directory Object, Authentication Scheme Object, and either an Application, Domain, or Realm Object.
- User Store supported by Layer7 SiteMinder (such as Active Directory)

### Layer7 SiteMinder Policy Server Configuration

Before you set up SiteMinder on Privileged Access Manager, configure these objects in the SiteMinder Administrative UI.

1. Create an Agent.
  - a. On the Infrastructure menu, select Agent, then Agents on its submenu. Select the Create Agent button on the right.  
Select OK to accept the option "Create a new object of type Agent."
  - b. For Name, enter the Fully Qualified Domain Name of the host Privileged Access Manager.
2. Create an Agent Configuration Object.
  - a. On the Agent menu, select Agent Configuration Objects. Select the Create Agent Configuration button.
  - b. Select the option "Create a copy of an object of type Agent Configuration." The `ApacheDefaultSettings` object is selected by default. Select OK.
  - c. Enter a Name for the agent configuration object.

### NOTE

Use the value of the Name field in the Privileged Access Manager SiteMinder configuration.

- d. Of the many Parameters that are displayed, only these parameters change:

- **AgentName:** Enter the Name of the Agent object that is created in Step 1. Select OK.
  - **DefaultAgentName:** Enter the Name of the Agent object that is created in Step 1. Select OK.
  - **HttpsPorts:** Enter the Privileged Access Manager HTTPS port, such as 443.
  - **GetPortFromHeaders:** Enter yes.
  - **LogoffUri:** Enter the Logoff page, such as "/logoff.php".
- e. Select **Submit**.
3. Create or modify an existing Host Configuration Object.
- a. Under the Hosts menu, select Host Configuration Objects.
  - b. Select Create Host Configuration to create one, or edit one by clicking the pencil opposite its Name field. For example, use `DefaultHostSettings`.

#### NOTE

Use the value of the Name field in the Privileged Access Manager SiteMinder configuration.

- c. Ensure that the Host address for the Policy Server field is the IP address of the Policy Server.
  - d. Select Submit.
4. Create a Directory Object.
- a. Under the Directory menu, select User Directories.
  - b. Select the Create User Directory button on the right.
  - c. Complete the following fields, according to your customer environment.
    - In the Name field, enter a name for the user directory.
    - In the Server field, enter the IP address and port.
    - In the Administrator Credentials section, select Require Credentials.
    - In the Username, enter a user DN who has at least read access to the user directory. For example: `CN=test,OU=Administrators,OU=IT,CN=doejo01`
    - Enter the password for this user in the Password and Confirm Password fields.
    - In the LDAP Settings section, set the LDAP Search Root, enter a DN. For example: `OU=Administrators,DC=company,DC=inc`
    - Under LDAP User DN Lookup, for Start, enter "(sAMAccountName=".
    - In the End field, enter ")".
    - Under User Attributes, set the Universal ID field as "sAMAccountName".
    - In the Disabled Flag field, enter "carLicense".
    - In the Password field, enter "unicodePwd".
    - In the Password Data field, enter "audio".
  - d. Select the Submit button.
5. Create an Authentication Scheme Object.
- a. Under the Authentication menu, select Authentication Schemes. Select the Create Authentication Scheme button on the right.
  - b. Select the option "Create a new object of type Authentication Scheme."
  - c. Complete the following fields:
    - In the Name field, enter `HTMLForm`.
    - In Authentication Scheme Type, select HTML Form Template.
    - In the Scheme Setup section, select Use Relative Target.
    - For Target, enter `/siteminderagent/forms/pamlogin.fcc`.
    - Accept the default values for the remaining fields.
  - d. Select submit.
6. Set up an Application, Domain, or Realm Object.

Depending upon how you want to protect your resources, select Application, Domain, or Realm. In this example, we demonstrate setting up an Application Object. We show how to set up protection for Privileged Access Manager. For more information about setting up these objects, see the Layer7 SiteMinder documentation.

- a. Under the Policies menu, select Application, Applications. Select the Create Application button on the right.
- b. Complete the following fields:
  - In the Name field, enter Privileged Access Manager.
  - In the Component Name field, enter Privileged Access Manager for our example.
  - In the Resource Filter field, enter **/cspm/home** for our example.
  - In the Default Resource Protection field, select Protected.
  - In the Authentication Scheme field, select **HTMLForm**.
  - Select Lookup Agent/Agent Group.
  - Select the Agent that you created in Step 1 (the Fully Qualified Domain Name of the host Privileged Access Manager). Select OK.
  - Select the Add/Remove button in the User Directories section.
  - Select the User Directory object that you created in Step 4. Select the arrow to move it to the Selected Members panel. Select OK.
  - Select the Resources tab, and select the Create button.
    - In the Name field, enter Privileged Access Manager for our example.
    - In the Resource field, enter **\***.
    - In the Action field, select Get and Post.
    - Select OK.
  - Select the Roles tab, and select the Create button.
    - Select "Create a new object of type Role." Select OK.
    - In the Name field, enter All Users.
    - For "Role applies to", select All Users.
    - Select OK.
  - Select Submit to create the Application object.
  - In the Applications panel, edit Privileged Access Manager by clicking the pencil icon.
  - Select the Policies tab.
    - Select the box for All Users under the Roles column, in the Privileged Access Manager row.
- c. Select submit.

## **Privileged Access Manager Configuration**

### **NOTE**

For a clustered environment, configure this on each cluster member.

Once the Layer7 SiteMinder Policy Server configuration steps are complete, follow these steps on Privileged Access Manager.

1. On the **Configuration** menu, select **Symantec Modules, SiteMinder**.
2. Add a Policy Server by clicking **+** under Policy Servers.
  - Enter the IP Address and Port. Use either IPv4 or IPv6 address.
3. Enter the **Policy Server Username**.
4. Enter the **Policy Server Password**.
5. Enter the **Host Configuration Object** from the SiteMinder setup, such as **DefaultHostSettings**.
6. Enter the **Agent Configuration Object** from SiteMinder setup.

**Note:** If this setting is incorrect, it causes the resource that is protected by this integration to become inaccessible. See [Use Console in Emergency](#) for more information.

7. Enter the **Trusted Host Name**. This name is used to register the SiteMinder Policy Server with Privileged Access Manager.
8. Select a **FIPS Mode**.  
This setting corresponds to one of the three Federal Information Processing Standard (FIPS) modes in which Layer7 SiteMinder operates:
  - **COMPAT**  
FIPS-compatibility mode uses algorithms existing in previous versions of Layer7 SiteMinder to encrypt sensitive data to maintain compatibility.
  - **MIGRATE**  
FIPS-migration mode enables you to transition from FIPS-compatibility mode to FIPS-only mode.
  - **ONLY**  
FIPS-only mode ensures that the Agent only accepts session keys, Agent Keys, and shared secrets that are encrypted using FIPS-compliant algorithms.
9. The read-only **SSO Enabled** checkbox indicates whether SiteMinder is enabled.
10. Select the **Save** button to save your configuration CA SiteMinder Web Agent and turn on Single Sign-On.
11. For the changes to take effect, select the **Restart Apache** button to restart the web server.
12. To test the SiteMinder feature, log in to Privileged Access Manager. Attempt to access the resource you are protecting. The SSO login screen appears. If the SSO login screen does not appear, the SSO integration has failed.
13. (Optional) **Disable**: If Layer7 SiteMinder integration is "Currently enabled," this button disables it.
14. The standard Layer7 SiteMinder login form has been modified for use with the main Privileged Access Manager frame. Select **Download Form** to download this form (pamlogin\_xx-XX.fcc). Alter it if necessary, and copy it to the desired location. Change the Target field value to the new form name and location.
15. To download the latest log file record of this instance of the Layer7 SiteMinder Web Agent, select **Download Log**. This file might be useful for troubleshooting if problems arise in the configuration of this CA module integration.

## **Troubleshooting**

### ***Use Console in Emergency***

If Privileged Access Manager is inaccessible, and you must disable SSO, use the Utility Console. If you have a VM, use an admin app such as vSphere to access the console. On the Console Main Menu, there is a new menu item for SSO. Select **Disable CA Single Sign-On**.

## **Known Issues**

### ***Agent Configuration Object Internal Server Error***

If an invalid Agent Configuration Object is specified, the web agent does not report an error. The user gets a success message and is prompted to restart. They do and then they cannot get back into Privileged Access Manager. They get this message:

#### **Internal Server Error**

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, or support.ca.com and inform them of the time the error occurred,

and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Additionally, a 500 Internal Server error was encountered while trying to use an ErrorDocument

to handle the request.



To enter Privileged Access Manager in this situation, disable SSO with the Utility Console. If you have a VM, use an admin such as vSphere to access the console. On the Console Main Menu, there is a new menu item for SSO. Select **Disable CA Single Sign-On**.

### **Client Failure**

When using the Privileged Access Manager Client to connect to your Privileged Access Manager instance, use the FQDN rather than the IP address. The Fully Qualified Domain Name succeeds, but the IP address fails without raising an error.

## **Integrate A2A Applications**

The concept of *request integration* refers to the process of replacing the hard-coded user names and passwords in an application with Credential Manager credential requests. This application is a “requesting application” or “requestor.”

The request integration process involves the following steps:

1. [Set up your Environment for Integration](#)
2. [Request Integration Algorithm](#)
3. Add your requestor to Credential Manager. See [Add A2A Requestors](#).
4. Adding an authorization mapping to Credential Manager. See [Add A2A Authorization Mappings](#).

### **Set Up Your Environment for Integration**

**Follow these steps:**

1. Install the A2A Client. See [Install an A2A Client for Credential Management](#).
2. Do the setup steps that are specific to your integration environment:
  - For a UNIX environment, source the **.cspmclicentrc** file or set up the environment variables that are contained within the file. The **.cspmclicentrc** file is located in: `$CSPM_CLIENT_HOME/cspmclicent/bin`.
  - For Microsoft Visual Studio, you do not need to register the DLL. It was done during A2A client installation.
  - For Eclipse, add the **capamclient.jar** file to the build path. This allows Eclipse to compile your application. See the procedure that is described in [Set Up Eclipse for A2A Integration](#).

### ***Set Up Eclipse for A2A Integration***

Use the following procedure to add the **capamclient.jar** file to the build path.

**Follow these steps:**

1. Open the project **Properties** dialog.
2. Select **Java Build Path**.
3. Select the **Libraries** tab.
4. Select **Add External JARs**.
5. Browse to the `$CSPM_CLIENT_HOME/cspmclicent/lib` folder and select the **capamclient.jar** file.
6. Close the **Properties** dialog.

### **Request Integration Algorithm**

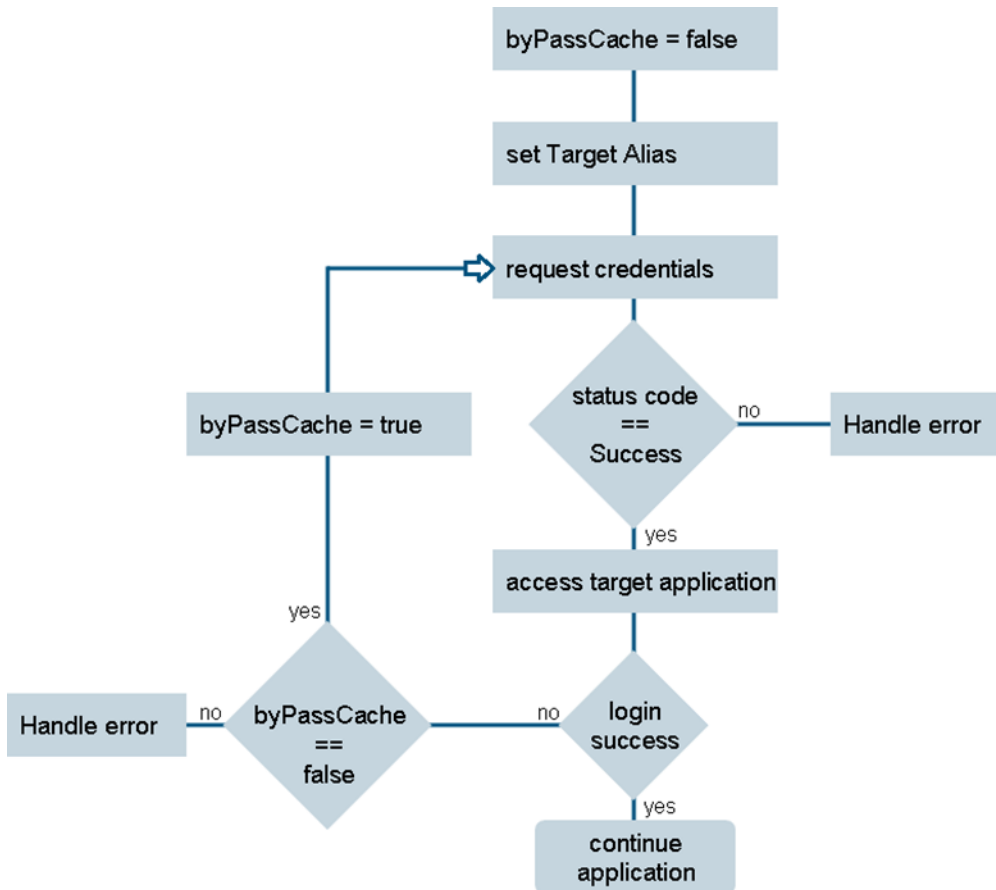
"Request integration" is the process of modifying your existing requestor to use Credential Manager to retrieve credential information instead of using hard-coded user names and passwords.

Integration methods for implementing the credential request are described in [Integrate Applications with the Credential Manager A2A Client](#).

Typically, when you integrate your application or script with the A2A client, you use the cached version of the credential. However, the supplied credentials only give the requestor access to the data if the A2A client cache is up-to-date. The following algorithm uses the cached credentials for the first login attempt. If the login fails the A2A client cache is

overridden, credentials are retrieved directly from the appliance, and a second login is attempted. By using the cached credentials for the first login attempt, you reduce the load on the appliance and improve performance. However, if the cached credential has gone stale, it can potentially incur a failed login attempt.

A failed login attempt can trigger an auditable security incident and possibly an account lockout condition if the number of failed login attempts exceeds the maximum that the policy allows.



## Integrate with SailPoint

- **SailPoint STI (Simple Table Integration)**  
STI is an extensive SailPoint-specific integration, with configuration required on both sides, resulting in automatic synchronization and workflow. This option requires an integration license option. See the following [STI Setup](#) section.
- **SCIM (System for Cross-domain Identity Management)**  
SCIM is an application-level REST protocol for managing user identity data between domains. The PAM REST API includes a SCIM section, including several undocumented SailPoint-specific extensions. For information about enabling the REST API, see [Connect with SCIM API](#). For information about the SCIM standard, see <http://www.simplecloud.info/>. For information about the SailPoint side of the integration, see the [SailPoint](#) documentation. The STI configuration is not necessary when using SCIM.

### Clustering

When Privileged Access Manager is clustered, users should connect to the cluster Primary Site VIP rather than an individual server. The VIP address provides availability in case the server that was originally configured for SailPoint is unavailable.

## STI Setup

Privileged Access Manager populates SailPoint integration tables with Privileged Access Manager Users (with current Role and User Group assignments), Roles, and User Groups. Privileged Access Manager Roles and User Groups are imported by SailPoint to be defined as Entitlements. Privileged Access Manager Users are imported and made into IdentityIQ Users in SailPoint. Whenever changes occur within Privileged Access Manager, these tables are updated on a configurable interval.

### Configuration

For the SailPoint configuration options to appear, the SailPoint integration option must be licensed. SailPoint STI uses port 3306 to communicate with PAM.

To configure SailPoint integration in Privileged Access Manager, follow these steps:

1. Go to **Configuration, 3rd Party, SailPoint**.
2. Enter the **Database User**, and **Database Password**. The password is used in SailPoint configuration, which follows.
3. Set the **Update Interval**, in seconds. This value determines how often Privileged Access Manager checks for incoming SailPoint requests, exports relevant data to SailPoint.
4. For **SailPoint Whitelist**, enter at least one SailPoint server address. These addresses are the only connections to allow for SailPoint integration. Valid entries are IP address, hostname, and FQDN values.
5. Select **Save** to save your settings.
6. Select **Install** to set up the SailPoint integration Tables. The installation is only done once. This button is enabled if SailPoint is licensed, and disabled again once the installation is complete.
7. Select **Download** to acquire a zip file of the Privileged Access Manager SailPoint application. Use this file during the configuration of the SailPoint side of the integration. Unzip this file and save CAPamConfiguration.xml in a location accessible by your SailPoint application.
8. The **Import** button is optional. You can manually direct Privileged Access Manager to read the provisioning queue. Import is also automatically done according to the Update Interval setting.
9. The **Export** button is optional. You can manually direct Privileged Access Manager to populate the SailPoint tables. Export is also automatically done according to the Update Interval setting.

### SailPoint Configuration

Before you configure the integration in SailPoint IdentityIQ, ensure that these prerequisites are met:

- Install the LCM (Lifecycle Manager) module for SailPoint
- Install the STI (Simple Table Integration) integration for SailPoint

To configure the integration in SailPoint, follow these steps:

1. In SailPoint IdentityIQ, select the configuration gear icon and select **Global Settings**. The Global Settings page appears.
2. Select the **Import from File** option in the lower right.
3. Select **Choose File** under **Import Objects**. Select CAPamConfiguration.xml, which you downloaded during the Privileged Access Manager configuration.
4. Select **Import**.
5. Under **Applications, Application Definitions**, select the **CAPam** application. The **Edit Application CAPam** page appears.
6. Select the Configuration tab.
7. Under **Settings**, enter the correct **Connection Password**, which was not provided in the configuration XML file. This password is the password that you entered in step 2 of [Privileged Access Manager Configuration](#).
8. Scroll down to **Object Type: usergroup**. Under **Settings**, enter the correct **Connection Password**.
9. Scroll down to **Object Type: role**. Under **Settings**, enter the correct **Connection Password**.
10. Scroll down to **Object Type: group**. Under **Settings**, enter the correct **Connection Password**.

11. Scroll to the bottom of the page and select **Test Connection**.  
"Test successful" appears. If not, edit the passwords.
12. Select **Save** to save your changes.

For your specific SailPoint IdentityIQ configuration, you can change the default provisioning policies that are provided by Privileged Access Manager. Inspect these settings to determine if you must change them.

1. Under **Configuration**, select **Provisioning Policies**.
2. Under **Object Type: account**, for the **Create** Type, select **User**.  
The **Attributes** for User appear.
3. Select an Attribute, such as **lastName**. See [Operations and Attributes](#) for a list of the supported operations and attributes.  
The **Edit Options** appear on the right.
4. Select **Value Settings**. The value for **lastName** can be a static Value, be Dependent, be determined by a Script, or be determined by a Rule.
5. If you want to save you changes, select **Save**.
6. On the **Edit Application CAPam, Password Policy** page, configure a default password policy that follows the default password policy set for Privileged Access Manager users.

### ***Operations and Attributes***

The following operations and attributes are supported for SailPoint integration. The listed attributes must be associated with a rule or value in a Provisioning Policy in the SailPoint **CAPam** application for attributes to sync. The **CAPam** application is configured with some default values, but clients might need to adjust these settings.

#### **Create a User**

To create a user with the "local " **authType**, all the listed attributes are required. To create a user with the "cac " **authType**, none of the listed attributes are required.

- **firstName**: User first name
- **lastName**: User last name
- **email**: User email address
- **password**: User password
- **authType**: supported values are **local** or **cac** (for smartcard users)
- **IIQDisabled**: **true** if user is disabled, or **false** if user is enabled
- **Roles** and **User Groups** are assigned as **Entitlements**.

#### **Modify a User**

To modify a user, all attributes are optional.

- **firstName**: User first name
- **lastName**: User last name
- **email**: User email address
- **password**: User password
- **authType**: supported values are **local** or **cac** (for smartcard users)
- **IIQDisabled**: **true** if user is disabled, or **false** if user is enabled
- **Roles** and **User Groups** are assigned or removed as **Entitlements**.

#### **Delete a User**

- No attributes

### ***Aggregation Tasks***

As part of the **CAPam** application setup in SailPoint, aggregation tasks are defined to SailPoint to collect the user and entitlement data from Privileged Access Manager. These tasks should be scheduled to execute regularly to keep this data in sync with Privileged Access Manager.

Follow these steps:

1. From the main SailPoint menu, select **Setup, Tasks**.  
Two Tasks are set up by the initial configuration:
  - **CAPam Account Aggregation** regularly reads the Privileged Access Manager User table to keep in sync with Users and their entitlements
  - **CAPam Group Aggregation** reads Privileged Access Manager User Roles and Groups and creates SailPoint Entitlements from them.
2. To schedule a task, right-click and select **Schedule** from the drop-down list to display the New Schedule dialog.
3. Select the **Scheduled Tasks** tab to edit schedules. You can select the **Run Now** box on the **Edit Schedule** tab to run the Task immediately.
4. To see a list of SailPoint entitlements, go to the main menu, **Applications, Entitlement Catalog**.

### **Workflow Example**

Once everything is configured in Privileged Access Manager and SailPoint IdentityIQ, the following example of the integration workflow is valid. This example shows a SailPoint user making a provisioning request for a Privileged Access Manager user.

1. In SailPoint, go to **Home**, and select **Manage User Access**.  
An IdentityIQ user list appears under the **Select Users** tab.
2. Select a User and select the **Manage Access** tab.
3. Select **Filters** on the right.  
The **Filter Access** panel appears.
4. From the **Entitlement Application** drop-down list, select **CAPam**, and **Apply**.  
The Roles and User Groups that are imported from Privileged Access Manager appear as Entitlements.
5. Select a User Group or Role as an Entitlement. Select the **Review** tab at the top of the page.
6. If the listed **Add Access** Entitlements are correct, select **Submit** at the bottom of the page.  
The Home page appears with a Success message at the top of the page.
7. SailPoint send this data to Privileged Access Manager as a provisioning request.
8. In Privileged Access Manager, go to **Users, Manage Users**, and find the new (or updated) User.  
The User should have the matching information, including Roles and Groups, as applicable.
9. The User should be able to log in to Privileged Access Manager with the appropriate entitlements.
10. An Aggregation Task runs in SailPoint, reading the information in the Privileged Access Manager integration tables,  
This Task closes the loop on the operation.

### **Activity Log**

The **Activity Log** displays information about every action pertaining to the SailPoint integration. Create, delete, and update actions, their source, time, and results are listed. To view the Activity Log, follow these steps:

1. Go to **Configuration, 3rd Party, SailPoint**.
2. Select the **Activity Log** tab.
3. The log table is sortable by clicking column headings. You can filter data using the controls above the headings.  
The **Info** column provides error messages, if applicable.

# Programming

The content in this section describes how to use the following APIs to create applications that interact with Privileged Access Manager:

- [External API](#) – A REST API that allows custom applications to configure and provision Privileged Access Manager.
- [Credential Manager CLI](#) – A command-line interface (CLI) that allows you to enter Credential Manager commands, or scripts of commands, from a command line.
- [Credential Manager Java API](#) – A Java API that provides access to Credential Manager capabilities from a Java program.

## PAM External REST API

The Privileged Access Manager External REST API provides programmatic control over most operations involving provisioning and granting access. These operations include managing users, devices, and policies.

External REST API access is over an HTTPS connection. Data is sent and received in the form of a JSON response. For more information about JSON, see <http://www.json.org/>.

This topic describes the following information:

### Deploying and Using the External REST API

Before programmers can use the External REST API, an administrator has to deploy and enable the API. After the API is enabled, programmers can implement API calls into their own programs.

Go to the appropriate procedures for your role in your organization:

- [Deploy the External REST API \(Administrators\)](#)
- [Use the External REST API \(Programmers\)](#)

### Use the API Explorer to View Dynamic External REST API Reference Information

Administrators and authorized users can explore the External REST API using the *API Explorer* that you access in the PAM UI by navigating to **Settings, API Doc**. The API Explorer allows you to view all API resources that are available for external use and the methods that are associated with them.

#### **NOTE**

The API Explorer is not available until the External REST API has been deployed.

### URIs for the External REST API

Each REST URI for the External REST API has *one* of the following formats:

- **CSPM URI:** `/cspm/ext/rest/resource_name/`  
Complete URL: `https://capam_hostname or ip_address/cspm/ext/rest/resource_name`
- **PHP URI:** `/api.php/v1/resource_name.json`  
`resource_name` represents an object or entity that you are managing through HTTP requests.

These URIs are only part of the REST URLs. To see the complete URLs, which include parameters and other values, see the **API Doc** in the UI.

**Example:** REST call to the `/cspm/ext/rest` endpoint. This call lists the global settings configuration properties:

```
GET https://111.12.32.1/cspm/ext/rest/configProperties
```

**Example:** REST call to the `/api.php/` endpoint. This call retrieves the user with an ID of 55.

```
GET https://111.12.32.1/api.php/v1/users.json/55
```

## Deploy the External REST API (Administrators)

Learn how to deploy the External REST API to provide programmatic control over most PAM functions.

As an administrator, use the procedures in this topic to enable the External REST API and configure who can use it.

### Enable the External REST API

External REST API capability is licensed by default. You cannot remove this capability. However, it is disabled by default.

Enable the External REST API to allow external calls to the appliance and to allow access to the online API Explorer documentation.

#### **Follow these steps:**

1. In the PAM UI, navigate to **Configuration, Security, Access**.
2. Next to the **External REST API** option, select **Enabled**.
3. Select **Save**.  
A confirmation message displays at the top of the page. Also, a message is written to the session logs.
4. Log out from the UI then log back in for all changes to take effect.

The External REST API methods are now available to calls from the battery the development of user applications and the **Try it out!** button of each method in the API Explorer documentation (**Settings, API Doc** in the UI):

### Grant External REST API Access to Users

To access the External REST API, a user requires a unique identifier that is called an *API key* that you assign and configure in its [account definition](#). The API key provides a password for authentication and role assignments that determine its privileges.

When the External API is invoked to execute a particular method, the API challenges for credentials using Basic authentication, requiring the assigned API key name and password in response. The API key is secured using HTTPS. When permissions are checked for the invoked method, the privileges that are associated with that particular API key are used.

To assign an API key to a user, follow *one* of these methods:

- [Add API Keys Using the UI](#)
- [Import API keys from a CSV file](#)

#### **Add API Keys Using the UI**


Add API keys in the PAM UI.

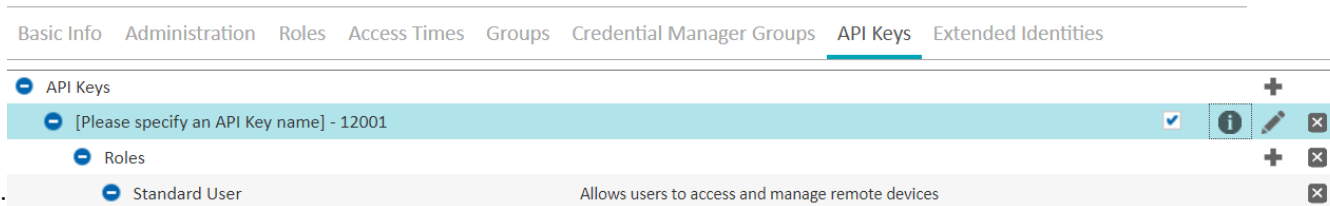
#### **Follow these steps:**

1. Log in to the UI and navigate to **Users, Manage Users**.
2. Open the user record of the user that you want that you want to authorize to make API method calls.
3. Select the **API Keys** tab.








4. Complete the following steps for each API key that you want to add:

- a. Select the **Add** icon () in the blue **API Keys** row at the top. A new entry opens, as shown in the following



example:

- b. Select the **Please Specify an API Key name** field and overwrite the text with a name for the API key. The name cannot contain whitespace. PAM appends a unique number. Consider the following information:
- A check symbol () in a checkbox across from the key name indicates that the key is active. To deactivate the key, select the box.
  - By default, the roles for the API key are the same roles that are assigned to the user account, including roles that are inherited from user groups of which the user is a member. Therefore, if you do not change the API Key role assignments (see Step C), the user can use the API to perform every function that they can do in the PAM UI.
  - To see roles inherited from user groups, select the **View inherited roles** icon (). The inherited roles are displayed in a dialog box.
- c. (Optionally) Do one or more of the following operations to modify existing roles:
- Select the **Add** icon () on the **Roles** line to add a role that is a subset of an existing role that is assigned to the user.  
For example, if the user is a Global Administrator, you can add any role that has privileges that the Global Administrator has. Similarly, if the user is a Delegated Administrator, only the roles that contain privileges that the Delegated Administrator has are available to add. If you select a role that requires permissions the user does not have, the API returns a warning that indicates that the API key has permissions that the user does not. If you receive this warning, remove the role.
- NOTE**  
You can assign roles to an API key that relies on privileges that are inherited from the groups of which the user is a member. However, if the user is removed from the group, the API key stops working.
- To remove an existing role, select the **Delete** icon () to the right of the role entry.
  - To remove roles that are inherited from a user group or groups, select the **Select User Group** icon () and deselect those groups in the dialog that opens.
- d. When you are finished modifying API keys, select **OK**.

### Import API Keys from a CSV File

You can prepare API keys in a comma-separated values (CSV) file and then import the file into the appliance database. If you do not have your own file, you can download a sample file. You can also import a CSV file exported from an existing PAM environment.

#### NOTE

Starting in PAM 4.1.6, the CSV definition for API keys includes a new `groupNames` attribute that allows you to specify from which user groups (of which the user is a member) an API key inherits roles.



In releases before 4.1.6, API keys inherited all roles from user groups of which the user was a member. When you import a CSV file that is exported from a release before 4.1.6, PAM reproduces the existing behavior by configuring all defined API keys to inherit from all user groups associated with the user.

#### Follow these steps:

1. Navigate to **Users, Manage Users**.
2. Select the **Import/Export** button.
3. To use the sample file as the starting point for preparing API key definitions, select **Download Sample File**, download the file (`UsersImportSample.csv`) and continue to Step 4.  
To import an existing CSV file, skip to Step 6.
4. Open the `UsersImportSample.csv` file, which contains a sample definition for a single API key:  
`"name=SampleApKey/;isActive=t/;description=Sample Api Key/;groupNames=DevMgrs|UserMgrs/;roles="`
5. Add values in the **API Keys** column, as required. Each entry must be represented by a concatenation of fields, as shown in the following excerpt. Bolded text highlights the parameters.

```
name=apikey1_name/;isActive=[t|
f]/;description=apiKey1_description/;groupNames=user_group1|user_group2/;roles=rolename=role_name1 roleUserGroups=[
f]/;description=apikey2_description/;groupNames=role_inheritance_groups/;roles=rolename=role_name1/;roleUserGroups=
rolename=role_name2
```

The delimiters for the API key entries are:

"	If multiple keys are assigned to one user, insert a double-quote character before and after the full string.
/;	Insert a forward slash and colon between each pair of fields for a key.
	Insert a pipe between user group names.
, rolename	If there are multiple roles for one key, insert a space followed by a comma between each pair of roles.
#&	Insert hash and ampersand between each pair of keys.

The following example shows two API key entries for a user:

```
name=apikey123/;isActive=t/;description=APIkey 123 description=Pre-poluated
API key/;groupNames=user_group1|user_group2/;roles=roleName=Service
Manager/;roleUserGroups=roleDeviceGroups=, roleName=Password Manager roleUserGroups=All
roleDeviceGroups=All#&name=apikey876/;isActive=t/; description=APIkey 876/; groupNames=Group1|
Group2/;roles=roleName=Service Manager roleUserGroups= roleDeviceGroups=, roleName=Password Manager
roleUserGroups= roleDeviceGroups="
```

6. Do the following steps to import a newly created or existing CSV file:
  - a. Select **Users, Manage Users, Import/Export**.
  - b. Select **Choose File** and browse to the CSV file.
  - c. Select **Import Users (User Groups)**.

#### View API Key Accounts and Policies

After you save a user record with newly added API keys, the appliance automatically creates the following objects:

- A target account. The name of the target account takes the format *API Key-UserID*. You can view the target accounts by navigating to **Credential Manager, Manage Targets, Accounts**. The following graphic shows an example:

<input type="checkbox"/>	Account Name	Application Nan	Application Type	Host Name	Device Name	Account Type	Owner User Na	Verified	Action
<input type="checkbox"/>	Test-API-3	ApiKey	Xsuite API Key	apikey.xceedium.com	apikey.xcee...	A2A			

**WARNING**

The Application Type **1.6Xsuite API Key** application type is only for use with the External REST API. Do not create any additional target applications of Application Type="Xsuite API Key".

- A policy for the user and the External REST API virtual device. The device has the default name [apikey.xceedium.com](http://apikey.xceedium.com). From the policy, you can view the password for the API key. A user can view the API Key name and password from the Access page in the UI. See [Obtain API keys](#).

**Deactivate or Delete an API Key**

To make an API key unavailable to its associated user, deactivate or delete the key. Navigate to **Users, Manage Users** then select the **API Keys** tab. Complete either of the following tasks:

**Deactivate:** To deactivate an API key for later use, clear the checkbox across from the API key name.

**Remove:** To remove an API key, select the **x** across from the API Key name.

**Disable the Test Button for API Methods (Optional)**

In the API Explorer, a button labeled **Try it out!** at the bottom of each API method description allows users to test API calls. The button is highlighted in the following example.

## roles

GET /api.php/v1/roles.json

### Implementation Notes

Retrieves the access roles defined in the system.

### Parameters

Parameter	Value	Description
fields	<input type="text" value="roleId,roleName,roleDescription,userFilter,deviceFilt"/>	The list of fields to return for each retrieved role data. Specify * to return all fields.
roleName	<input type="text"/>	Filter the returned roles by their names.

### Response Messages

HTTP Status Code	Reason	Response Model
200		

Try it out!



You can test an API after applying variable settings, and it returns output to the documentation interface. This test mechanism accesses actual data and can change data in the live Privileged Access Manager database.

If you do not want users to have this ability, you can hide the **Try it out!** Button (for all users).

#### To hide the button:

1. From the UI, go to the **Global Settings, Basic Settings**
2. Clear the **External REST API Buttons** checkbox. (**Enable** is checked by default.)

After you enable the API, permit users access to the API by assigning API keys.

## Use the External REST API (Programmers)

You can review and test the External REST API methods before using these methods with a production application.

Complete the following tasks to use the External REST API with your applications:

## Obtain an API Key

To perform any API operation, you must authenticate with the External REST API. The External REST API authenticates users with HTTP Basic authentication. When you are challenged for credentials, provide an API key and password that a PAM Administrator has assigned to you.

### NOTE

If an administrator deactivates your user account, the appliance deactivates the API key.

After your Administrator assigns you an API key, obtain your API key credentials so you can test API methods. Retrieve the credentials from one of two places:

- [Access page](#)
- [Target account](#)

### Follow these steps:

1. In the UI, navigate to the **Access** page.
2. For the `apikey.xceedium.com` device, select the pull-down menu from the icon under the **Target Applications** column. Select the key name, `Test-API-3` in this example screen, to display the account name and password.

Device Name	Address	Operati	Access Methods	Web Portal	RDP Applications
apikey.xceedium.com	apikey.xceedium.com	Other			

3. Note these values somewhere then select **Close**.

When you test an API method for the first time, you are prompted to enter credentials. Specify the API account name and password. You can now test the API methods in the API Explorer.

From a target account, follow these steps:

1. In the UI, navigate to the **Credentials, Manage Targets, Accounts**. The list of accounts displays.
2. For the API account, select the View icon under the **Action** column to view the account name and the password.

<input type="checkbox"/>	Account Name	Application Name	Application Type	Host Name	Device Name	Account Name
<input type="checkbox"/>	Test-API-3	ApiKey	Xsuite API Key	apikey.xceedium.com	apikey.xcee...	A2A

The **Show Password** screen displays.

3. Note these values somewhere then select **Close**.

When you test an API method for the first time, you are prompted to enter credentials. Specify the API account name and password. You can now test the API methods in the API Explorer.

### NOTE

The appliance appends a number to the API key name that matches the User ID. The number ensures that the key name is unique for each user. For example, if the API key name is `Test-API` and the User ID is `3`, the appliance appends `-3` to the name. The result is `Test-API-3`.

## Reset the Active API Key

To change which API keys are available to you, follow the action for the interface to the UI.

- Web browser: Clear the browser cache and execute a new API call.
- CA PAM Client: Log out and log back in. Execute a new API call.

When you execute the next API call, you are prompted for API key credentials.

### View API Methods in the API Explorer

You can view each External REST API method using the API Explorer. Each method is presented with a description and its syntax. You can also test an API method with varying parameters. API method test calls are executed against the Privileged Access Manager database. Messages and responses are returned only for the fields that are shown in the Explorer.

#### Follow these steps:

1. Select **Settings, API Doc**.
2. The **API Explorer** opens and lists all the API resources available. To the right of each resource, you can filter the display using the options:
  - **Show/Hide** – Toggles the display for that resource.
  - **List Operations** – Displays a list of the API methods in that category.
  - **Expand Operations** – Displays parameter details for all API methods in that category.

You can also select any resource to see the methods. The following sample shows the **/devices** resource with the **get /api.php/v1/devices.json/{id}** expanded. Open or close the methods by selecting the method name itself.

GET
/api.php/v1/devices.json/{id}
Retrieve the device with the specified id.

#### Implementation Notes

Retrieve the device with the specified id. GET {id}

#### Parameters

Parameter	Value	Description	Parameter Type	Data Type
id	(required)	The id of the device.	path	undefined
fields	deviceId,deviceName,domainName,description,os,t	The list of fields to return for the retrieved device. Specify * to return all fields.	query	string

#### Response Messages

HTTP Status Code	Reason	Response Model	Headers
200			

Try it out!

The display shows the following sections:

- Implementation Notes – Describes the API function.
- Parameters – Describes each input parameter. Populate required fields to test a response.
- Response Messages - Describes the HTTP response.

### Test API Requests

After you enter parameters for a method, select the **Try it out!** button at the bottom of the page to test the method call. Use any parameter inputs from the fields in the API Explorer. Most API methods accept standard parameters and API-specific parameters. The parameters can affect how a request is handled and how a response is formatted.

A response displays with the following information:

- Curl - Shows the URL request using cURL format.
- Request URL – Displays the URL submitted to for API method call processing.
- Response Body – Displays the JSON structure returned.
- Response Code – Displays the HTTP status codes returned.
- Response Headers – Displays the response fields of the HTTP transaction.

The full set of parameters and their descriptions is in the **API Doc** interface. All parameters are optional except where noted. To exclude an optional parameter, leave it out from the request or include it with an empty value.

#### TIP

If you have a user role with the necessary permissions, you can hide the **Try it out!** button so that no operations can be performed on active settings. See [Disable the test button](#).

#### *Example: Test attributes for a Single User*

##### Follow these steps:

1. Under the **users** resource, select the method **get api.php/v1/users.json{id}**. This method retrieves information about a specific user.
2. Populate the **id** field with the account name for the API key, such as Test-API-3. If you do not know the account name, see [Obtain API Keys](#).
3. Make any needed edits to the requested attributes list in the **fields** field.
4. Select **Try it out!**  
If this method is the first one you are trying in this session, the API prompts you for the API Key credentials.
5. Enter your credentials.
6. If your credentials are correct and the parameters are valid, you receive a successful response. If the request fails for some reason, you receive error feedback.

#### Use the External REST API in a Clustered Environment

In a clustered environment, use the primary VIP for bulk operations.

Load balancers can use health.php to determine the node status. If you are using external load balancers in a clustered environment, set the External REST API URLs to use the load balancers URLs. See [Configure Load Balancers to Determine the Availability of Cluster Nodes](#) for details.

#### External API Example Implementation

The following code excerpt shows a PHP example in curl using External API methods. The example provisions a user, a device, and the auto-connection policy between the two. You can work with CA Technologies Professional Services to prepare client software that can access Privileged Access Manager with API requests.

```
<?php
class APIConstants{
    const DEVICE_ENDPOINT_V1 = "/api.php/v1/devices.json";
    const DEVICE_GROUP_ENDPOINT_V1 = "/api.php/v1/devicegroups.json";
    const GET = "GET";
    const POLICIES_ENDPOINT_V1 = "/api.php/v1/policies.json";
    const ROLE_GLOBAL_ADMINISTRATOR = 1;
    const ROLE_STANDARD_USER = 2;
    const ROLE_OPERATIONAL_ADMINISTRATOR = 14;
```

---

```

const POST = "POST";
const PUT = "PUT";
const TWO_DAYS = 172800;
const USER_ENDPOINT_V1 = "/api.php/v1/users.json";
const USER_GROUP_ENDPOINT_V1 = "/api.php/v1/userGroups.json";
}
/**
 *
 * This function will make a single request to the API.
 * @param string $apiKey - api key name and password delimited by colon
 * @param string $url - the URL to reach the desired endpoint of the API.
 * For a get may include parameters
 * @param string $postData - JSON encoded set of parameters
 * @param string $httpOperation - GET, POST, PUT, or DELETE
 * @return string -1 for failure, otherwise results of request
 */
function makeAPIRequest($apiKey, $url, $postData = null, $httpOperation) {
    global $debug;
    $httpOperation = strtoupper($httpOperation);
    if(!in_array($httpOperation,array("GET","POST","PUT","DELETE"))){
        return -1;
    }

    /*
        In real code the url could be validated. This is left out as a distraction
        to the point of the cookbook.
    */

    if(!empty($postData) && is_null(json_decode($postData))){
        error_log("Invalid post data " . print_r($postData,true) .
            "\n Post data must be in JSON format.");
        return -1;
    }

    // apiKey must have at least one colon, and not in the first position
    if(strpos($apiKey,":") == 0){
        error_log("Incorrectly formatted api key. Key must consist of api key name, a
colon, and the api password");
    }

```

```

        return -1;
    }

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
    curl_setopt($ch, CURLOPT_TIMEOUT, 30);
    curl_setopt($ch, CURLOPT_HTTPAUTH, CURLAUTH_ANY);
    curl_setopt($ch, CURLOPT_USERPWD, $apiKey);
    switch($httpOperation){
        case "GET":
            break;
        case "PUT":
            curl_setopt($ch, CURLOPT_CUSTOMREQUEST, "PUT");
            // absence of break is intentional
        case "POST":
            curl_setopt($ch, CURLOPT_POST, true);
            curl_setopt($ch, CURLOPT_POSTFIELDS, $postData);
            curl_setopt($ch, CURLOPT_HTTPHEADER,
                array('Content-Type: application/json', 'Content-Length: ' .
strlen($postData)));
            break;
        case "DELETE":
            curl_setopt($ch, CURLOPT_CUSTOMREQUEST, "DELETE");
    }
    /*
    * These are useful debug statements
    */
    if($debug){
        echo "XXX: URL = " . $url . PHP_EOL;
        echo "YYY: parameters = " . print_r($postData, true) . PHP_EOL;
        echo "ZZZ: httpOperation = " . $httpOperation . PHP_EOL;
    }
    $data = curl_exec($ch);
    if($debug){
        echo "AAA: return = " . print_r($data, true) . PHP_EOL;
    }

    $error = curl_error($ch);
    if(!empty($error)){
        error_log("CURL request to $url returned error: $error");
    }

```



```

        $data = -1;
    }

    curl_close($ch);
    return trim($data);
}

/* assume following parameters
 * argv[1] = URL component e.g, http://10.1.10.24/ port may be included
 * argv[2] = user name for REST API
 * argv[3] = password for REST API
 * argv[4] = first name of user to be provisioned
 * argv[5] = last name of user
 * argv[6] = email address of user
 * argv[7] = device name
 * argv[8] = domain name
 * argv[9] = operating system
 * argv[10] = user name for target account
 * argv[11] = debug 0 for false any positive for true
 */
if(count($argv) != 12){
    // in real code more information would be supplied
    echo " Missing required parameters. ". PHP_EOL;
    return ;
}
$baseUrl = $argv[1];
$apiKey = $argv[2]. ":" . $argv[3];
$firstName = $argv[4];
$lastName = $argv[5];
$email = $argv[6];
$device['deviceName'] = $argv[7];
$device['domainName'] = $argv[8];
$device['os'] = $argv[9];
$userAccountName = $argv[10];
$debug = $argv[11];

$username = $firstName . "_" . $lastName;

/*
 * Determine if the user already exists.
 * The user name has to be unique, but since all searches are 'contains ' style, add the
 * first and last names

```

```

* to reduce the number of substring hits. For this first example we will code the URL
manually
*/
$url = "https://" . $baseUrl . APIConstants::USER_ENDPOINT_V1 . "?
userName=" . urlencode($userName) .
"&firstName=" . urlencode($firstName) . "&lastName=" . urlencode($lastName) .
"&fields=userId,userName,expiration,roles";
$userData = makeAPIRequest($apiKey, $url, null, APIConstants::GET);
//the true in the decode parameter list makes the JSON be turned into PHP associative
arrays,
// rather than a mix of arrays and stdClass objects.
$userList = json_decode($userData,true);

/*
* if the user is not found, create it. Have it immediately active, but expiring in 48
hours
* from now
*/
if($userList['totalRows'] === 0){
    // The return from creating a new user is the id of the newly created user
    $userId = buildNewUser($userName,$firstName,$lastName,$email);
    // add error checking
    if($userId == -1){
        echo " Failed to add new user " . $userName . ". Aborting";
        return;
    }
}else{
    /*
    // if the user already exists then
    // update the expiration time by two days unless the expiration date is set to
unlimited or
    * later than 2 days away
    // add standard user to the list of roles if they don't already have the role
    */
    unset($user);
    foreach($userList['users'] AS $userCandidate){
        // There can be only one exact match on userName
        if($userCandidate['userName'] == $userName){
            // null is returned for a successful update
            $result = updateUser($userCandidate);
            if(!empty($result)){
                echo "Update failed with result " . print_r($result,true) . PHP_EOL;
            }
            $userId = $userCandidate['userId'];
            break;
        }
    }
}

```

```

    }
}

/*
// Add the user to a group, either to give it a desired set of privileges or
* to let the user have access to group level policies
*/
if(isset($userId)){
    addUserToGroup($userId, "Standard Role Users");
}

/* now to process the device. Do an OR search to find any devices that match either the
device name
* or the domain name
*/
$searchParameters = $device;
unset($searchParameters['os']);
// add extra fields to make device usable - assume typeAccess
$device['typeAccess'] = 't';
$deviceList = findDevice($searchParameters,"OR",

    "deviceId,deviceName,domainName,os,typePassword,typeAccess,deviceAccessMethods");
if(isset($deviceList['totalRows'])){

    // cases 0 matches - go ahead and create it
    switch($deviceList['totalRows']){
        case 0:
            $deviceId = buildNewDevice($device);
            $device['deviceId'] = $deviceId;
            // now add an access method
            $accessMethodId = updateDevice($device);
            break;
        case 1:
            // confirm both dom name and device name match
            // check for access method if missing add it.
            $deviceCandidate = $deviceList['devices'][0];
            if($deviceCandidate['deviceName'] == $device['deviceName'] &&
                $deviceCandidate['domainName'] == $device['domainName']){
                $accessMethodId = updateDevice($deviceCandidate);
                $deviceId = $deviceCandidate['deviceId'];
                $device['deviceId'] = $deviceId;
            }else{ // conflict

```

```

        echo "Device retrieved was " . $deviceCandidate['deviceName'] .
        " with a domain name of " . $deviceCandidate['domainName'] . PHP_EOL;
        echo "Device searched for was " . $device['deviceName'] .
        " with a domain name of " . $device['domainName'] . PHP_EOL;
        return -1;
    }
    break;
default:
    // find the device that has an exact hit if any and update it
    foreach($deviceList['devices'] AS $deviceCandidate){
        $foundDevice = false;
        if($deviceCandidate['deviceName'] == $device['deviceName'] &&
            $deviceCandidate['domainName'] == $device['domainName']){
            $accessMethodId = updateDevice($deviceCandidate);
            $deviceId = $deviceCandidate['deviceId'];
            $device['deviceId'] = $deviceId;
            $foundDevice = true;
            break;
        }
    }
    if(!$foundDevice){
        echo "Could not find device with name " . $device['deviceName'] .
        " and domain name of " . $device['domainName'] . PHP_EOL;
        return -1;
    }
}
}else{
    /*
    * problem with query
    */
    echo "Device retrieve query had a problem. Details were " .
    print_r($deviceList,true) . PHP_EOL;
    echo "Aborting." . PHP_EOL;
    return;
}

/*
* create a policy between the user and the device using the access method we added
*/
$policy = findExistingPolicy($userId,$deviceId);
if($policy === 0){
    $policyId = addPolicy($userId,$deviceId,$accessMethodId);
    /*
    * if we found a policy then we returned the details
    */
}

```

```

}elseif(is_array($policy)){
    $policyId = $policy['id'];
    /*
     * otherwise something went wrong
     */
}elseif ($policy == -1){
    return;
}

// check to see if a target application for this device already exists
$targetApplicationId = findTargetApplication($device);
/*
 * check to see if array returned, if so check for error code
 */
if(is_array($targetApplicationId)){
    foreach($targetApplicationId AS $errorMessage){
        /*
         * Message 5186 says Device not found or is not a target server.
         * Since the device must exist because we found it earlier, it must not be a
target server.
         * Update the device to be of typePassword (i.e., a target server).
         */
        if(strpos($errorMessage['message'], "5186")){
            $results = updateDeviceTargetServer($device['deviceId'], 't');
            /*
             * A successful update returns nothing.
             */
            if(empty($results)){
                $targetApplicationId = 0;
                break;
            }else{
                /*
                 * More error processing goes here
                 */
            }
        }
    }
}

if(empty($targetApplicationId)){
    /*
     * To demonstrate error handling we will try to add a target application despite the
fact that
     * the device is not typePassword
     */
    $targetApplicationId = addTargetApplication($device);
}

```

```

}
if(!is_numeric($targetApplicationId) || $targetApplicationId < 1){
    // error time to abort
    return;
}
// if needed add a target account for auto-connect to the target application
$targetAccountId = findTargetAccount($deviceId,$targetApplicationId,$userAccountName);
if(empty($targetAccountId)){
    $targetAccountId = addTargetAccount($deviceId,$targetApplicationId,
$userAccountName);
}

$policy = findExistingPolicy($userId,$deviceId);

if($policy === 0){
    $policyId = addPolicy($userId,$deviceId,$accessMethodId);
}elseif(is_array($policy)){
    $policyId = $policy['id'];
}elseif ($policy == -1){
    return;
}
// retrieve the policy again and add the target application for auto-connect
$policy = findExistingPolicy($userId,$deviceId);
addSSOToPolicy($policy,$accessMethodId,$targetAccountId);

function buildNewUser($userName,$firstName,$lastName,$email){
    global $apiKey, $baseUrl;
    // We can either use stdClass or an associative array to build POST or PUT data.
    // This example uses stdClass
    $user = new stdClass();
    $user->userName = $userName;
    $user->firstName = $firstName;
    $user->lastName = $lastName;
    $user->email = $email;
    $user->roles =
array(array("roleId"=>2,"userGroups"=>array(),"deviceGroups"=>array()));
    $user->password = "password";
    $user->expiration = time() + APIConstants::TWO_DAYS;
    $parameters = new stdClass();
    $parameters->data = $user;
    $addUrl = "https://" . $baseUrl . APIConstants::USER_ENDPOINT_V1;

```

---

```

        return makeAPIRequest($apiKey, $addUrl,
        json_encode($parameters),APIConstants::POST);
    }

/*
 * Another way to give users certain roles is to assign them to a user group with those
 * roles.
 * As an example we will get the id for a group called Standard Role Users
 * This example uses the php http_build_query function to generate the URL encoded
 * parameters
 */
function addUserToGroup($userId,$groupName) {
    global $apiKey,$baseUrl;
    $url = "https://" . $baseUrl . APIConstants::USER_GROUP_ENDPOINT_V1 . "?" .

http_build_query(array("groupName"=>
$groupName,"fields"=>"groupId,groupName,description"));
    $groupData = makeAPIRequest($apiKey, $url,null, APIConstants::GET);
    if($groupData == -1){
        echo "Failed to get user group list. User " .
        $userId . " will not be added to the Standard Role Users group" . PHP_EOL;
    }
    //the true in the decode parameter list makes the JSON be turned into PHP
    associative arrays,
    // rather than a mix of arrays and stdClass objects.
    $groupList = json_decode($groupData,true);

    if(isset($groupList['totalRows'])){
        switch($groupList['totalRows']){
            case 0:
                break;
            case 1:
                $groupId = $groupList['groups'][0]['groupId'];
                echo "groupId " . $groupId .PHP_EOL;
                break;
            default:
                foreach($groupList['groups'] AS $userGroup){
                    if("Standard Role Users" == $userGroup['groupName']){
                        $groupId = $userGroup['groupId'];
                        break 2;
                    }
                }
        }
    }
}

```

---

```

    }
    if(isset($groupId)){
        $url = "https://" . $baseUrl . APIConstants::USER_ENDPOINT_V1 . "/" .
            $groupId . "/users/" . $userId;
        $result = makeAPIRequest($apiKey, $url, null, APIConstants::POST);
    }
} else {
    echo "totalrows not found" . PHP_EOL;
}
}

function updateUser($userCandidate) {
    global $apiKey, $baseUrl;
    $user['userId'] = $userCandidate['userId'];
    $userId = $userCandidate['userId'];
    if(!empty($userCandidate['expiration'])){
        $newExpirationTime = time() + APIConstants::TWO_DAYS;
        $user['expiration'] = ($newExpirationTime > $userCandidate['expiration']) ?
            $newExpirationTime : $userCandidate['expiration'];
    }
    $addStandardUsers = true;
    if(count($userCandidate['roles']) > 0){
        foreach($userCandidate['roles'] AS $role){
            if(in_array($role['roleId'],
array(APIConstants::ROLE_STANDARD_USER, APIConstants::ROLE_GLOBAL_ADMINISTRATOR,
        APIConstants::ROLE_OPERATIONAL_ADMINISTRATOR))) {
                $addStandardUsers = false;
                break;
            }
        }
    }
    if($addStandardUsers){
        $user['roles'] = $userCandidate['roles'];
        $user['roles'][] = array("roleId"=>APIConstants::ROLE_STANDARD_USER,
            "userGroups"=>array(),
            "deviceGroups"=>array());
    }
    $updateUrl = "https://" . $baseUrl . APIConstants::USER_ENDPOINT_V1;
    $parameters['data'] = $user;
    $result = makeAPIRequest($apiKey, $updateUrl,
json_encode($parameters), APIConstants::PUT);
    return $result;
}

```



---

```

/**
 *
 * @param array $searchParms - keys are search fields value are values
 * @param string $searchRelationship AND or OR if there are multiple search parameters
 * @param string $fields what information about a device you want returned. NULL takes
 * the
 * default the API returns
 */
function findDevice(array $searchParameters,$searchRelationship="AND",$fields=null){
    global $apiKey,$baseUrl;
    $searchParameters['searchRelationship'] = $searchRelationship;
    if(!empty($fields)){
        $searchParameters['fields'] = $fields;
    }
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "?" .
        http_build_query($searchParameters);
    $deviceData = makeAPIRequest($apiKey, $url, null, APIConstants::GET);
    $deviceList = json_decode($deviceData,true);
    return $deviceList;
}

function findDeviceById($deviceId,$fields=null){
    global $apiKey,$baseUrl;
    if(!empty($fields)){
        $searchParameters['fields'] = $fields;
    }
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "/" . $deviceId;
}

/**
 * create a new device
 * @return deviceId (int)
 * @param array $device
 */
function buildNewDevice($device){
    global $apiKey,$baseUrl;
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1;
    $deviceId = makeAPIRequest($apiKey, $url,json_encode($device), APIConstants::POST);
    $device['deviceId'] = $deviceId;
    return $deviceId;
}

```

```

/**
 * Updates a device to add an access method.
 * @param array $device
 * @return access method id
 */
function updateDevice(array $device){
    global $apiKey,$baseURL;
    $addAccessMethod = true;
    if(!empty($device['deviceAccessMethods'])){
        foreach($device['deviceAccessMethods'] as $accessMethod){
            if((strtoupper($device['os']) == "LINUX" && $accessMethod['type'] == "SSH"
&&
                isset($accessMethod['id'])) ){
                return $accessMethod['id'];
            }
        }
    }
    /*
    * Always add SSH if one isn't there
    */

    $accessMethods = array(
        "type" => "SSH",
        "port" => 22
    );
    $url = "https://" . $baseURL . APIConstants::DEVICE_ENDPOINT_V1 . "/" .
        $device['deviceId'] . "/accessMethods";
    $parameters['accessMethods'] = array($accessMethods);
    $accessMethodJSON = makeAPIRequest($apiKey, $url, json_encode($parameters),
APIConstants::POST);
    /*
    * We know there is only one entry in the array at most
    */
    $accessMethod = json_decode($accessMethodJSON,true);
    $addedAccessMethod = $accessMethod[0];
    return $addedAccessMethod['id'];
}

/**
 * Add a UNIX type target application (Windows Domain/Proxy not supported, Generic too
simple)
 * @param array $device

```

```

*/
function addTargetApplication(array $device){
    global $apiKey, $baseUrl;
    $results = addUnixTargetApplication($device);
    if(is_numeric($results)){
        $targetApplicationId = $results;
    }else{
        $errors = json_decode($results,true);
        if(is_array($errors)){
            // More error processing here
            $targetApplicationId = -1;
        }
    }
    // either the actual target application id or -1 for failure to find or error
    message if one returned
    return $targetApplicationId;
}

/**
 *
 * @param array $device
 * @return mixed empty array if no target application found,
 * int the targetApplication id if found
 * array of error messages if found
 */
function findTargetApplication($device){
    global $apiKey,$baseUrl;
    // first see if the application already exists. Don't specify fields so as to take
    the default
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "/" .
    $device['deviceId'] . "/targetApplications";
    $parameter['data']['applicationName'] = $device['deviceName'] . " Unix account";
    $results = makeAPIRequest($apiKey, $url, json_encode($parameter),
    APIConstants::GET);
    $targetApplications = json_decode($results,true);
    // if an empty array was returned the search was successful and there were no
    matching target application.
    if(is_array($targetApplications) && !empty($targetApplications)){
        foreach($targetApplications AS $targetApplication){
            if(isset($targetApplication['id']) && $parameter['data']['applicationName']
            == $targetApplication['applicationName']){
                return $targetApplication['id'];
            }else if(!isset($targetApplication['id'])){ // error code returned
                echo " Error when trying to search for a target application. Error was
                " . print_r($targetApplications,true) . PHP_EOL;
            }
        }
    }
}

```

```

        // since there may be multiple error messages return everything, not
        just this error
        return json_decode($results,true);
    }
}
}

/**
 * Add a new target server of type Unix to the specified device
 * @param array $device
 * @return Ambiguous <string, number>
 */
function addUnixTargetApplication($device){
    global $apiKey,$baseUrl;
    $parameter['data']['applicationName'] = $device['deviceName'] . " Unix account";
    $parameter['data']['applicationType'] = "unixII";
    $attributes = array("sshSessionTimeout"=>60000,"sshPort"=>22,"unixVariant"=>"LINUX",
        "sshUseDefaultCiphers"=>"true");
    $parameter['data']['attributes'] = $attributes;
    /*
    * notice how we use exactly the same URL here as in findTargetApplication.
    * The only difference is that the type of transaction is POST.
    * The parameters are different, but that isn't part of the URL.
    */
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "/" .
    $device['deviceId'] .
        "/targetApplications";
    $results = makeAPIRequest($apiKey, $url, json_encode($parameter),
    APIConstants::POST);
    return $results;
}

/**
 * change a device to either be of typePassword (t) or not (f)
 * @param integer $deviceId
 * @param string $trueOrFalse
 */
function updateDeviceTargetServer($deviceId,$trueOrFalse){
    global $apiKey, $baseUrl;
    // obviously check if $trueOrFalse is t or f
    $parameter['data']['typePassword'] = $trueOrFalse;
    $parameter['data']['deviceId'] = $deviceId;

```

---

```

    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1;
    $results = makeAPIRequest($apiKey, $url, json_encode($parameter),
APIConstants::PUT);
}

/**
 * Find a target account for a particular target application (and hence for a particular
 device)
 * @param integer $deviceId
 * @param integer $targetApplicationId
 * @param string $accountName
 * @return mixed - id if successful, error messages if not
 */
function findTargetAccount($deviceId, $targetApplicationId, $accountName){
    global $apiKey, $baseUrl;
    // same thing - check if target account exists already
    $parameter['data']['accountName'] = $accountName;
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "/" . $deviceId .
"/targetApplications/" . $targetApplicationId . "/targetAccounts";
    $targetAccountResults = makeAPIRequest($apiKey, $url, json_encode($parameter),
APIConstants::GET);
    $targetAccounts = json_decode($targetAccountResults, true);
    if(is_array($targetAccounts)){
        foreach($targetAccounts as $targetAccount){
            if($targetAccount['accountName'] == $accountName){
                return $targetAccount['accountId'];
            }
        }
    }
    return $targetAccounts;
}

/**
 *
 * @param int $deviceId
 * @param int $targetApplicationId
 * @param string $accountName
 * @return Ambiguous <string, number> int if successful add otherwise
 */
function addTargetAccount($deviceId, $targetApplicationId, $accountName){
    global $apiKey, $baseUrl;

```

---

```

    $parameter['data']['accountName'] = $accountName;
    // special code to tell PA to generate a unique password based on password
composition policy
    $parameter['data']['password'] = "generate_pass";
    $parameter['data']['useAliasNameParameter'] = 't';
    $parameter['data']['aliasNames'] = $accountName . ",alias" . $accountName;
    $url = "https://" . $baseUrl . APIConstants::DEVICE_ENDPOINT_V1 . "/" . $deviceId .
"/targetApplications/" . $targetApplicationId . "/targetAccounts";
    $results = makeAPIRequest($apiKey, $url, json_encode($parameter),
APIConstants::POST);
    if(!is_numeric($results)){
        // decode if this is a JSON string
        $checkResults = json_decode($results, true);
        if(!empty($checkResults)){
            $results = $checkResults;
        }
    }
    return $results;
}

```

```

/**
 *
 * @param int $userId
 * @param int $deviceId
 * @return policy object if found, 0 if no policy, -1 if invalid parameters
 */
function findExistingPolicy($userId,$deviceId){
    global $apiKey, $baseUrl;
    $url = "https://" . $baseUrl . APIConstants::POLICIES_ENDPOINT_V1 . "/" . $userId .
"/" . $deviceId ."?fields=id,accessMethods";
    $results = makeAPIRequest($apiKey, $url, null, APIConstants::GET);
    $policy = json_decode($results,true);
    if(isset($policy['id'])){
        return $policy;
    }
    // most likely results are some kind of error message
    if(is_array($policy) && count($policy) > 0){
        foreach($policy AS $message){
            // Message 12033 - userid and device id were both valid, but no policy
between them exists
            if(strpos($message['message'], "12033") !== false){
                return 0;
            }
            // Message 12034 - user or group id specified in policy does not exist
            if(strpos($message['message'], "12034") !== false){

```

```

        echo $message['message'] . PHP_EOL;
        return -1;
    }
    // Message 12035 - device or group id specified in policy does not exist
    if(strpos($message['message'], "12035") !== false){
        echo $message['message'] . PHP_EOL;
        return -1;
    }
    // unexpected error
    echo $message['message'] . PHP_EOL;
    return -1;
}
}
}
/**
 * Add a policy between a user and a device for an access method, without specifying
 * auto-connection.
 * @param integer $userId
 * @param integer $deviceId
 * @param integer $accessMethodId
 * @return policy id on success else void
 */
function addPolicy($userId, $deviceId, $accessMethodId) {
    global $apiKey, $baseUrl;

    $url = "https://" . $baseUrl . APIConstants::POLICIES_ENDPOINT_V1 . "/" . $userId .
    "/" . $deviceId;
    $accessMethods = array(array("accessMethodId"=>$accessMethodId));
    $parameter['accessMethods'] = $accessMethods;
    // turn on cli recording
    $parameter['cliRecording'] = "t";
    $results = makeAPIRequest($apiKey, $url, json_encode($parameter),
    APIConstants::POST);
    if(is_numeric($results)){
        return $results;
    }
}
/**
 * Replace the existing access method for the policy with one that has a target account
 * for auto-connection.
 * @param array $policy
 * @param integer $accessMethodId
 * @param integer $targetAccountId
 */
function addSSOToPolicy($policy, $accessMethodId, $targetAccountId) {

```

```

global $apiKey, $baseUrl;
/**
 * Multiple target accounts could be assigned, so the accountIds are an array
 */
$putData = array(array("accessMethodId"=>
$accessMethodId,"accountIds"=>array($targetAccountId)));
$url = "https://" . $baseUrl . APIConstants::POLICIES_ENDPOINT_V1 . "/" .
$policy['id'] .
"/accessMethods";
$results = makeAPIRequest($apiKey, $url,json_encode($putData),APIConstants::PUT);
}

```

## Connect with SCIM API

SCIM is an application-level REST protocol for managing user identity data between domains. The PAM REST API includes a SCIM section. For information about enabling the PAM REST API, see [PAM External REST API](#). For information about the SCIM standard, see <http://www.simplecloud.info/>.

For information about SailPoint and SCIM, see [Integrate with SailPoint](#). SailPoint SCIM access with REST API uses port 443.

### SCIM Methods

A selection of supported SCIM 2.0 API methods follows. For complete documentation of the API, use the [API Doc](#).

#### Get

ResourceTypes	Retrieve all SCIM Resource Types or for a specific ID.
Schemas	Retrieve all SCIM schema or for a specific ID.
Groups	Retrieve all SCIM User Groups or for a specific ID.
Users	Retrieve all SCIM Users or for a specific ID.
ServiceProviderConfig	Retrieve SCIM Service Provider Configuration.

#### Post

Groups	Add new SCIM User Group.
Groups/.search	Search for a SCIM User Group.
Users	Add new SCIM User.
Users/.search	Search for a SCIM User.

#### Put

Groups/{id}	Update a SCIM User Group.
Users/{id}	Update a SCIM User.



**Delete**

Groups/{id}	Delete a SCIM User Group.
Users/{id}	Delete a SCIM User.

**LDAP External REST API Extensions**

The PAM LDAP update task is performed automatically by the LDAP periodic update daemon. The following REST API extensions give users more explicit control over the process of synchronizing PAM with the corresponding LDAP information.

The API Doc section of the PAM UI, which includes the REST API test facility, contains an abbreviated version of this content.

**NOTE**

See [Use the External API \(Programmers\)](#) for information about enabling the external API and accessing the API Doc.

LDAP import/update processing for all domains is performed on the first member of the primary site. Only one import/update process can be running at any time. To avoid API call conflicts and failures, follow this best practice procedure:

1. In a clustered environment, use the LDAP REST APIs:
  - Ensure that the cluster is on. Otherwise, HTTP Error 503 (Service Unavailable) is returned.
  - The APIs can be invoked only against the Primary site.
  - Secondary sites return this message in the JSON response: "PAM-CM-1786: This API operation is not available from a secondary site."
2. Disable the periodic update process for all configured LDAP domains using one of the following methods:
  - Make changes in the UI: Go to **Configuration, 3rd Party, LDAP, LDAP Domains, Update Domain, Disable Periodic Update**.
  - Invoke the REST API: [PUT /cspm/ext/rest/ldap/refresh](#)
3. Ensure that no other LDAP update job is running. This rule applies to both automatic and API-triggered updates. You can either:
  - Wait for the current job to complete
  - Use the REST APIs to test ([GET /cspm/ext/rest/ldap/refresh](#)) and abort ([DELETE /cspm/ext/rest/ldap/abort](#)) the current job.
4. Invoke REST APIs to perform the required updates of LDAP-imported groups. You can use either:
  - [PUT /cspm/ext/rest/ldap/userGroup](#)
  - [PUT /cspm/ext/rest/ldap/deviceGroup](#)
5. Enable the periodic update process for LDAP domains that you do not want to control using the REST API.
  - Once disabled, the update process is not automatically enabled by the system.
  - The periodic LDAP domain update is controlled separately for each configured LDAP domain.

**NOTE**

**NOTE:** The searches that are performed by this REST API are not case-sensitive.

**GET /cspm/ext/rest/ldap/refresh**

Test whether an LDAP job is running.

**URL:**

`https://<PAM>/cspm/ext/rest/ldap/refresh`

**Parameters:**

- none -

**Response:**

JSON, job is running:

```
{
  "data": null,
  "success": true,
  "total": 1,
  "message": null
}
```

JSON, job is not running:

```
{
  "data": null,
  "success": true,
  "total": 0,
  "message": "PAM-CM-1784: LDAP Refresh is not in progress."
}
```

**POST /cspm/ext/rest/ldap/userGroup**

Create a new PAM LDAP user group and import its users.

**URL:**

`https://<PAM>/cspm/ext/rest/ldap/userGroup`

**Parameters:**

Parameter	Required	Values	Description
groupDn	Yes		Domain name or common name for the LDAP group or Organizational Unit to be imported to PAM.
domainDn	Yes		Base domain name for the domain to which this group belongs.
authenticationType	Yes	ldap / ldap+rsa / ldap+radius / pki / radius / rsa / saml / tacacs+	Authentication method used by users in the group. The method must be configured on the PAM appliance.

**Response**

JSON:

```
{
  "data": null,
```

```

"success": true,
"total": 1,
"message": null
}

```

**success\_value:**

"true" if the LDAP creation process completed successfully,

"false" otherwise (For example, if interrupted, errors, warnings, and so on).

**Note:** Warnings and Errors in each data response set have to be inspected to make the determination of the overall operation outcome.

**total:**

Contains the number of groups processed (successfully or not).

**message:**

May contain error text indicating the source of failure.

**POST /cspm/ext/rest/ldap/deviceGroup**

Create a new PAM LDAP device group and import its devices.

**URL**

<https://<PAM>/cspm/ext/rest/ldap/deviceGroup>

This API has the same structure as [/cspm/ext/rest/ldap/userGroup](#) but applies to LDAP-imported devices.

**Parameters**

Parameter	Required	Values	Description
groupDn	Yes		Domain name or common name for the LDAP group or Organizational Unit to be imported to PAM.
domainDn	Yes		Base domain name for the domain to which this group belongs.

**Response**

JSON:

```

{
  "data": null,
  "success": true,
  "total": 1,
  "message": null
}

```

**success\_value:**

"true" if the LDAP refresh process completed successfully,

"false" otherwise (For example, if interrupted, errors, warnings, and so on).

**Note:** Warnings and Errors in each data response set have to be inspected to make the determination of the overall operation outcome.

***total:***

Contains the number of groups processed (successfully or not).

***message:***

May contain error text indicating the source of failure.

**PUT /cspm/ext/rest/ldap/refresh**

Enable or disable the LDAP periodic refresh process.

This API mimics the function of the UI switch in the **Configuration, LDAP, LDAP Domains, Update Domain, Disable Periodic Update** section of the UI.

**URL:**

`https://<PAM>/cspm/ext/rest/ldap/refresh?baseDN=dnValue&disableRefresh=drValue`

**Parameters:**

[required] `domainName` :

`dnValue` specifies the LDAP DN of the domain for which to set the switch controlling the refresh.

The refresh of each LDAP domain that is configured in Privileged Access Manager is controlled separately.

[required] `disableRefresh` :

`drValue` is either "true" to disable the periodic refresh process, or "false" to enable it.

**Response:**

JSON, success:

```
{
  "data": null,
  "success": true,
  "total": 1,
  "message": null
}
```

JSON, failure:

```
{
  "data": null,
  "success": true,
  "total": 0,
  "message": "PAM-CM-1785: No change. LDAP Disable Refresh switch is already in the requested state."
}
```

**PUT /cspm/ext/rest/ldap/userGroup**

Refresh the indicated LDAP-imported user groups.

**URL:**

<https://<PAM>/cspm/ext/rest/ldap/userGroup?groupNamesList=gnList>  
<https://<PAM>/cspm/ext/rest/ldap/userGroup?groupNamesLike=gnLike>  
<https://<PAM>/cspm/ext/rest/ldap/userGroup?groupNamesList=gnList&dryRun=drValue>  
<https://<PAM>/cspm/ext/rest/ldap/userGroup?domainName=dnValue&groupNamesList=gnList>  
<https://<PAM>/cspm/ext/rest/ldap/userGroup?domainName=dnValue&groupNamesLike=gnLike>

**Parameters:**

Parameter	Required	Values	Description
domainName	No		dnValue specifies the LDAP DN of the domain from which to select the user groups to refresh. If not provided, all available LDAP domains are checked for the specified groups to refresh.
groupNamesList	Yes*		A semicolon-separated list of DNs of user groups to refresh. For example: OU=ITC_OU2, DC=qapam, DC=local
groupNamesLike	Yes*		A SQL LIKE expression to use while selecting the DNs of the user groups to process. For example: %OU=Info %OU=Contract%
dryRun	No	true/false	If "true", the API prepares and verifies the user group names that are specified by other parameters, but it does not submit them to the Appliance for processing. This parameter can be used with any combination of the other parameters.

\*Either groupNamesList or groupNamesLike parameter is required.

**Response**

JSON:

```

{
  "data": [
    {
      "numberOfNewMembers": 0,
      "numberOfUpdatedMembers": 0,
      "groupDN": "group 1 name",
      "numberOfProcessedMembers": 2,
      "warnings": [],
      "connectionFailure": false,
    }
  ]
}
```

```

    "numberOfFailedAddMembers": 0,
    "numberOfFailedUpdateMembers": 0,
    "numberOfDeletedMembers": 0,
    "numberOfFailedDeleteMembers": 0,
    "errors": []
  },
  ...
],
"success": success_value,
"total": number-or-groups-processed,
"message": null
}

```

**data:**

Contains the array result sets, one set for each processed group.

Each set comprises properties describing the result of group update.

**NOTE**

If `connectionFailure` is "true", data set may not contain the usual complement of properties.

**success\_value:**

"true" if the LDAP refresh process completed successfully,

"false" otherwise (For example, if interrupted, errors, warnings, and so on).

**Note:** Warnings and Errors in each data response set have to be inspected to make the determination of the overall operation outcome.

**total:**

Contains the number of groups processed (successfully or not).

**message:**

May contain error text indicating the source of failure.

**PUT /cspm/ext/rest/ldap/deviceGroup**

Refresh the indicated LDAP-imported device groups.

**URL**

`https://<PAM>/cspm/ext/rest/ldap/deviceGroup?groupNamesList=gnList`

`https://<PAM>/cspm/ext/rest/ldap/deviceGroup?groupNamesLike=gnLike`

`https://<PAM>/cspm/ext/rest/ldap/deviceGroup?groupNamesList=gnList&dryRun=drValue`

`https://<PAM>/cspm/ext/rest/ldap/deviceGroup?domainName=dnValue&groupNamesList=gnList`

`https://<PAM>/cspm/ext/rest/ldap/deviceGroup?domainName=dnValue&groupNamesLike=gnLike`

This API has the same structure as `/cspm/ext/rest/ldap/userGroup` but applies to LDAP-imported devices.

## Parameters

Parameter	Required	Values	Description
domainName	No		dnValue specifies the LDAP DN of the domain from which to select the device groups to refresh. If not provided, all available LDAP domains are checked for the specified groups to refresh.
groupNamesList	Yes*		A semicolon-separated list of DNs of device groups to refresh. For example: OU=ITC_OU2, DC=qapam, DC=local
groupNamesLike	Yes*		A SQL LIKE expression to use while selecting the DNs of the device groups to process. For example: %OU=Info %OU=Contract%
dryRun	No	true/false	If "true", the API prepares and verifies the device group names that are specified by other parameters, but it does not submit them to the appliance for processing. This parameter can be used with any combination of the other parameters.

\*Either groupNamesList or groupNamesLike parameter is required.

## Response

JSON:

```
{
  "data": [
    {
      "numberOfNewMembers": 0,
      "numberOfUpdatedMembers": 0,
      "groupDN": "group 1 name",
      "numberOfProcessedMembers": 2,
      "warnings": [],
      "connectionFailure": false,
      "numberOfFailedAddMembers": 0,
      "numberOfFailedUpdateMembers": 0,
      "numberOfDeletedMembers": 0,
      "numberOfFailedDeleteMembers": 0,
      "errors": []
    },
    ...
  ]
}
```

```

],
"success": success_value,
"total": number-or-groups-processed,
"message": null
}

```

**data:**

Contains the array result sets, one set for each processed group.

Each set comprises properties describing the result of group update.

**NOTE**

If `connectionFailure` is "true", data set may not contain the usual complement of properties.

**success\_value:**

"true" if the LDAP refresh process completed successfully,

"false" otherwise (For example, if interrupted, errors, warnings, and so on).

**Note:** Warnings and Errors in each data response set have to be inspected to make the determination of the overall operation outcome.

**total:**

Contains the number of groups processed (successfully or not).

**message:**

May contain error text indicating the source of failure.

**DELETE /cspm/ext/rest/ldap/abort**

Abort the current LDAP group refresh.

Invoking this API aborts current LDAP refresh process, either periodic or triggered by the API.

**URL:**

```
https://<PAM>/cspm/ext/rest/ldap/abort
```

**Parameters:**

- none -

**Response:**

JSON, job canceled:

```

{
  "data": null,
  "success": true,
  "total": 0,
  "message": null
}

```

JSON, job not canceled:

```

{
  "data": null,

```



```

"success": false,
"total": 0,
"message": "PAM-CM-1784: LDAP Refresh is not in progress."
}

```

## Credential Manager CLI and Credential Manager Java API

Credential Manager has two programming interfaces that you can use for password management functions:

- **Command-line interface (CLI):** The Credential Manager CLI enables programmatic access to the password management functions of the Credential Manager. The CLI also provides access to a limited set of maintenance operations. You can issue a command, or a script of commands, from a Windows or UNIX/Linux command line. The [Credential Manager CLI Commands](#) describe all the available commands.
- **Java API:** The Java API gives access to Credential Manager capabilities from a Java program. The Java API provides you with a mechanism to integrate Credential Manager with your Java programs. The Java API is supported on the UNIX/LINUX and Windows platforms. The cliTool.jar file also contains the Javadocs that describe each available Java API command.

For each interface, the commands available to a user depend on the roles and groups that are assigned to the user in the PAM UI.

Install the CLI and the Java API on any client system, then connect this remote system to the Privileged Access Manager appliance across an HTTPS network connection. From the client system, issue CLI or Java API commands to administer the Credential Manager information programmatically.

### NOTE

The client must be able to establish a secure (HTTPS) connection to the appliance.

This section provides information about the Java API and the CLI.

**Use the table of contents to access the topics in this section.**

## Install and Set Up the Remote CLI and Java API

To use the remote CLI or the Java API, install and configure the software on a client system in your environment. The client system is remote to the PAM appliance, and it is the system that you plan to use to manage Credential Manager.

Complete the following procedures on the client system connecting to Privileged Access Manager.

### NOTE

Complete these instructions whether you plan to use the Remote CLI, the Java API, or both.

### Download and Deploy the Remote CLI Software

Follow this procedure to download and deploy the appropriate version of the Remote CLI software, which is packaged as a zip file, to your client system. The release version of the Remote CLI software should be the latest available version corresponding to the PAM release running on your appliance.

### **Follow these steps on the client system:**

1. Download the Windows Proxy software from the Broadcom Support site. For information on how to download the software, see [Download PAM Installation Media](#).
2. Create a directory on the local system and extract the contents of the zip file into it.  
The following files are extracted:

- **cliTool.jar**
  - **capam\_command.bat** (for CLI access from a Windows system)
  - **capam\_command** (for CLI access from a UNIX/Linux system)
3. (Optionally) For convenience, add the installation directory to your `PATH`.
  4. Do one of the following steps:
    - For UNIX/Linux systems, identify the installation directory by entering `export CAPAM_DIR =installation_directory`.
    - For Windows systems, add an Environment Variable named `CAPAM_CLI` with the value of the path to the installation directory. For example: `C:\CA\CAPAM\CLI_32`
  5. If it is not already installed, install the Java Runtime Environment (JRE) Version 8u-latest. Obtain the JRE from <https://adoptopenjdk.net>. If you are creating a Java application that uses the Java API, you also need the Java Version 8 SDK.

### **Enable the Credential Manager CLI**

**Follow these steps to enable the remote CLI:**

1. Connect to the PAM appliance using a browser or the CA PAM Client.
2. Navigate to **Configuration, Security, Access**
3. On the Access page, select the **Enabled** radio button that is associated with the **Credential Management CLI** entry.
4. Select **Save**.
5. Navigate to **Settings, Credential Manager**.
6. Verify that the **Enable External CLI** option is enabled. If not, enable it and restart the appliance.

### **Obtain a Certificate**

CLI and Java API commands must be executed over an HTTPS connection between your client system and the PAM appliance. To secure the connection, obtain a certificate that the client trusts.

Complete the following steps to obtain a certificate:

1. [Gather Information for the certificate](#)
2. [Generate a certificate or use an existing certificate](#)
3. [Apply the certificate](#)
4. [Create a keystore](#)

#### **NOTE**

To complete the steps for getting a certificate, connect to the appliance using a browser or the CA PAM Client.

### ***Gather Information for the Certificate***

Gather the following information for each PAM appliance before generating a certificate:

- IP address or the internal VIP for appliances in a cluster
- Fully qualified domain name (FQDN)
- FQDN short name: If the fully qualified domain name is `jdoe@ca.com`, the short name is `jdoe`.

### ***Generate a Certificate or Use an Existing Certificate***

Use a certificate from a Certificate Authority or use a self-signed certificate to secure the network connection. If the PAM appliance already has a certificate available, skip to [Generate a keystore](#).

#### **WARNING**

Do not use the default certificate, `gkcert.crt`, or a certificate that has no Alternate Subject Names.

**Follow these steps to obtain a certificate:**

1. From your client system, log in to the PAM UI from a web browser or using the CA PAM Client.
2. Select **Configuration, Security, Certificates, Create**.

The following screen shows the Certificates page:

**Certificates**

Create Upload Download Set CRL Options Sign Applets

Type ☒ Self-Signed Certificate ☐ CSR

Key Size: \* 2048 ▼

Common Name: \*

Country: \*

State:

City:

Organization: \*

Org. Unit:

Days: \* 365 ▲▼

Alternate Subject Names:

Filename: default

CREATE

3. Select the one of the appropriate options:
  - **Self-signed Certificate**
  - **CSR** to request a certificate from a Certificate Authority
4. Complete the fields in the form. Add the appliance information that you gathered to the **Alternate Subject Names** box. Add one name or IP address per line.
5. After the form is complete, select **Create**.  
If you completed a CSR, download the CSR and then send the request to a Certificate Authority. The Certificate Authority signs and returns a certificate, which you must upload to the appliance. Use the **Upload** tab on the Certificates page.
6. Set and accept the certificate:
  - a. Select the **Set** tab.
  - b. Pick the certificate in the **Filename** field.
  - c. Select **Verify Certificate**. A confirmation message displays at the top of the page.
  - d. Select **Accept Certificate**.

**WARNING**

Accepting the certificate forces the appliance to reboot.

7. After the reboot, apply the certificate.

## Apply the Certificate

If you are using a PAM-generated certificate, download it to your client system. If you are using a Certificate Authority-obtained certificate, upload it from your client system to the PAM appliance.

Complete *one* of the procedures for your certificate:

### If you obtained a certificate from the PAM appliance:

1. Select the **Download** tab.
2. In the **Filename** field, select the certificate from the pull-down list.  
A password for the certificate is not required.
3. Select **Download**.
4. When prompted, save the certificate to the directory where you installed the cliTool.jar file.

### If you obtained a certificate from a Certificate Authority:

1. Select the **Upload** tab.
2. For the Type option, select **Certificate**
3. In the **Filename** field, browse for the certificate on your client system.
4. **Fill in any other required fields.**
5. Select **Upload**.

Go to the next section to generate a keystore on your client system.

## Create a Keystore

Generate a keystore on the client system. This keystore must contain the certificate from the client system. You can generate a keystore in many ways. The following steps explain only *one* method, using the keytool utility.

### Follow these steps for the keytool utility:

1. Navigate to the directory where you put the cliTool.jar file.
2. Generate the keystore and import the certificate to this keystore. Use the following command but note the guidelines:
  - You can substitute capam.crt for another file name with the .crt extension.
  - Do not change the keystore name. It must be **capam.keystore**
  - You must place the **capam.keystore** file in the same folder as the cliTool.jar file. If keytool is executed directly in the Java bin directory, you must manually copy the resulting **capam.keystore** file to the same folder as cliTool.jar.

#### UNIX/Linux:

```
$JAVA_HOME/bin/keytool -import -trustcacerts -file capam.crt -alias capamserver -
keystore capam.keystore
```

**Note:** starting in JRE 1.8, **-import** is replaced by **-importcert**

#### Windows:

```
%JAVA_HOME%\bin\keytool -import -trustcacerts -file capam.crt -alias capamserver -
keystore capam.keystore
```

**Note:** starting in JRE 1.8, **-import** is replaced by **-importcert**

- After you execute the command, you are prompted for the keystore password. Enter a new password for the keystore you are creating. The following messages display:

```
Trust this certificate? [no]: yes
```

```
Certificate was added to keystore
```

- Verify that the import is successful by listing the keystore contents:  
UNIX/Linux:

```
$JAVA_HOME/bin/keytool -list -v -keystore capam.keystore
```

Windows:

```
%JAVA_HOME%\bin\keytool -list -v -keystore capam.keystore
```

### **Verify the Installation**

To verify that the installation works, execute a command. For example:

```
capam_command capam=forwardinc.com adminUserID=admin cmdName=getErrorCodes
```

If successful, a list of error codes displays. The host name (forwardinc.com) must match the server name in the certificate. If the certificate contains an IP address for the appliance, you can use the address in place of the server name.

Before the command executes, you are prompted for the Credential Manager administrator password. If the command executes successfully, it produces an XML string. For more information about the return values, see [Remote CLI Return Values](#).

## **Use the Credential Manager Java API**

To develop a program using the Java API, add the cliTool.jar file as a build path dependency. The resulting Java program also has a runtime dependency on the cliTool.jar file.

To run a program that uses the Java API, ensure that the cliTool.jar file is part of the classpath. You access the Java API from a Java program by including the cliTool.jar in your project classpath.

### **NOTE**

The cliTool.jar file also contains the Javadocs that describe each available Java API command.

Use the following procedure to use the Java API to run CLI commands from your Java program.

### **Follow these steps:**

- Import the necessary classes. At a minimum, you require:

```
com.cloakware.cspm.common.AdminAPICommandNames
com.cloakware.cspm.common.AdminAPIParameterNames
com.cloakware.cspm.server.ui.Request
```

```
com.cloakware.cspm.server.ui.AdminAPI com.cloakware.cspm.server.ui.Result
```

Base Model objects represent elements of the Credential Manager data model. They include all objects that are derived from the `BaseModel` class; such as `TargetAccount`, `TargetApplication`, `TargetServer`, `Role`, `Request`, `RequestScript`, and `RequestServer`.

```
import com.cloakware.cspm.common.AdminAPICommandNames; import
com.cloakware.cspm.common.AdminAPIParameterNames;

import com.cloakware.cspm.server.ui.Request; import
com.cloakware.cspm.server.ui.AdminAPI; import com.cloakware.cspm.server.ui.Result;
```

2. Instantiate the `AdminAPI` class by entering the following command:

```
AdminAPI adminAPI = new AdminAPI();
```

3. Log in to Privileged Access Manager using the following command. The Java API operates in a session-specific state, which requires you to log in to the appliance.

```
adminAPI.login(locationOfKeystore, userId, password);
```

The roles and groups that are assigned to a user determine which CLI commands a user can execute CLI. The user must have the password management role. The group Operational Administrator is sufficient to execute CLI commands, and group "System Admin Group" contains full privileges to execute password management CLI commands.

4. Perform your CLI commands. You can run CLI commands by:

- Creating a request object and applying the `AdminAPI execute` method, or
- If the command involves a Base Model object, you can create an instance of the Base Model object and can run the `AdminAPI add`, `update`, or `delete` method.

For example, to add a target server using the request object and the `AdminAPI execute` method, enter the following commands:

```
Request myRequest = new Request();
myRequest.setCommand(AdminAPICommandNames.ADD_TARGET_SERVER);

myRequest.setParameter(AdminAPIParameterNames.ADD_TARGET_SERVER_HOST_NAME,
    "myhost.mycompany.com");

myRequest.setParameter(AdminAPIParameterNames.ADD_TARGET_SERVER_IP_ADDRESS,
    "12.12.12.12");

Result myResult = adminAPI.execute(myRequest); System.out.println("result: "+
    myResult.getStatusMessage());
```

For example, to add a target server using the `TargetServer` object and the `AdminAPI add` method:

```
myTargetServer.setHostName("myhost.mydomain2.com");
myTargetServer.setIPAddress("10.12.13.14");
```

```
Result myResult = adminAPI.add(myTargetServer); System.out.println("result: "+
    myResult.getStatusMessage());
```

## 5. When you are finished using the CLI, log out from the appliance:

```
adminAPI.logout();
```

### NOTE

More information: [Credential Manager Java API Example](#).

## Credential Manager Java API Example

The `javaAPIExample.java` helps you learn how to use the Java API.

This example is an implementation of a Java API-based application for use with Credential Manager.

```
import java.util.ArrayList;
import java.util.List;

import com.cloakware.cspm.common.AdminAPICommandNames;
import com.cloakware.cspm.common.AdminAPIParameterNames;
import com.cloakware.cspm.server.bo.Agent;
import com.cloakware.cspm.server.bo.Authorization;
import com.cloakware.cspm.server.bo.Filter;
import com.cloakware.cspm.server.bo.Group;
import com.cloakware.cspm.server.bo.PasswordPolicy;
import com.cloakware.cspm.server.bo.PasswordViewPolicy;
import com.cloakware.cspm.server.bo.RequestScript;
import com.cloakware.cspm.server.bo.RequestServer;
import com.cloakware.cspm.server.bo.Role;
import com.cloakware.cspm.server.bo.TargetAccount;
import com.cloakware.cspm.server.bo.TargetAlias;
import com.cloakware.cspm.server.bo.TargetApplication;
import com.cloakware.cspm.server.bo.TargetServer;
import com.cloakware.cspm.server.bo.User;
import com.cloakware.cspm.server.bo.UserGroup;
import com.cloakware.cspm.server.ui.AdminAPI;
import com.cloakware.cspm.server.ui.AdminAPIFactory;
import com.cloakware.cspm.server.ui.Request;
import com.cloakware.cspm.server.ui.Result;

/**
 * An implementation of a Java API based application.
 *
 * This program does not contain a complete list of commands and parameters.
 * Refer to the Java Documentation for the Password
 * Authority Java API or the CLI Documentation for the complete list.
 *
 * This program can be instantiated in your own program or can be executed
 * through the Command Line.
 *
 * The Password Authority cliTool.jar must be in your Class Path to
```

```
* use this application.
*
* This application should only be used in Password Authority version 4.2.1 or
* above and Java 1.5 or above.
*
*/

public class JavaAPIExample {

    private AdminAPI adminAPI;
    private Result result;
    private Request request;

    private String passwordAuthorityServerKeyStore =
        "C:\\Program Files\\CAPAM\\capam.keystore";
    private String passwordAuthorityUserName = "super";
    private String passwordAuthorityUserPassword = "admin4cspm!";
    private String passwordAuthorityServerHostName = "localhost";

    private TargetServer targetServer;
    private TargetApplication targetApplication;
    private TargetAccount targetAccount;
    private TargetAlias targetAlias;
    private RequestServer requestServer;
    private RequestScript requestScript;
    private Authorization authorization;
    private Group targetGroup;
    private Group requestGroup;
    private Role role;
    private UserGroup userGroup;
    private PasswordPolicy passwordPolicy;
    private PasswordViewPolicy passwordViewPolicy;
    private User user;

    //Target Server
    private static final String TARGET_SERVER_HOST_NAME =
        "hostname.cloakware.com";

    //Target Application
    private static final String TARGET_APPLICATION_NAME = "Target Application";
    private static final String TARGET_APPLICATION_TYPE = "unix";
    private static final String SSH_PORT_ATTRIBUTE = "sshPort";
    private static final String SSH_PORT = "22";

    //Target Account
    private static final String TARGET_ACCOUNT_USER_NAME = "username";
    private static final String TARGET_ACCOUNT_USER_PASSWORD = "password123!";
    private static final String USE_OTHER_ACCOUNT_TO_CHANGE_PASSWORD_ATTRIBUTE =
        "useOtherAccountToChangePassword";

    //Target Alias
```



```
private static final String TARGET_ALIAS_NAME = "targetAlias";

//Request Server
private static final String REQUEST_SERVER_HOST_NAME =
    "requestserver.cloakware.com";

//Request Script
private static final String REQUEST_SCRIPT_NAME = "example.pl";
private static final String REQUEST_SCRIPT_EXECUTION_PATH = "C:\\test";
private static final String REQUEST_SCRIPT_FILE_PATH = "C:\\test";
private static final String REQUEST_SCRIPT_TYPE = "Perl";

//Target Group
private static final String TARGET_GROUP_NAME = "targetGroup";

//Request Group
private static final String REQUEST_GROUP_NAME = "requestGroup";

//Filter
private static final String FILTER_EXPRESSION = REQUEST_SERVER_HOST_NAME;

//Role
private static final String ROLE_NAME = "roleName";
private static final String ROLE_ADD_REQUEST_SERVER = "addRequestServer";
private static final String ROLE_UPDATE_REQUEST_SERVER =
    "updateRequestServer";
private static final String ROLE_DELETE_REQUEST_SERVER =
    "deleteRequestServer";

//User Group
private static final String USER_GROUP_NAME = "userGroup";
private static final String USER_GROUP_DESCRIPTION = "userGroupDescription";

//User
private static final String USER_USER_NAME = "userName";
private static final String USER_USER_PASSWORD = "admin4cspm!";

//Password Policy
private static final String PASSWORD_POLICY_NAME = "passwordPolicy";
private static final String PASSWORD_POLICY_DESCRIPTION =
    "passwordPolicyDesc";
private static final int MINIMUM_PASSWORD_LENGTH = 3;
private static final int MAXIMUM_PASSWORD_LENGTH = 8;

//Password View Policy
private static final String PASSWORD_VIEW_POLICY_NAME =
    "passwordViewPolicy";

//View Target Account Password
private static final String VIEW_TARGET_ACCOUNT_USER_NAME = "admin";
private static final String VIEW_TARGET_ACCOUNT_USER_PASSWORD =
    "admin4cspm!";
private static final String VIEW_TARGET_ACCOUNT_REASON =
```

```

        "I need access to the server.";

//Update Agent
private static final int AGENT_ID = 1000;
private static final String AGENT_HOST_NAME = "test.ca.com";
private static final String AGENT_DEVICE_NAME = "WindowsProxyTestMachine";
private static final String AGENT_DESCRIPTOR1 = "Testing update agent";
private static final String AGENT_DESCRIPTOR2 = "Update windows proxy descriptor2";

/**
 * This application can be run with no arguments or the following:
 * key store - Password Authority Key Store
 * user - Password Authority user name
 * password - Password of the user
 * host name - Password Authority Server
 *
 * The order of the arguments is fixed, however the arguments are
 * themselves optional. If no arguments are provided, it
 * uses the default values of a new Password Authority Windows Server
 * Installation.
 *
 * @param args - The list of command line arguments.
 */
public static void main(String[] args) {
    JavaAPIExample javaAPIExample = new JavaAPIExample();

    javaAPIExample.init(args);
    javaAPIExample.runJavaAPIExample();
    javaAPIExample.logout();
}

/**
 * Initializes the Java API object and logs in to the Password Authority
 * Server. The String Array should contain the location of a Password
 * Authority key store, a Password Authority user name, the password of
 * that user, and the host name of a Password Authority Server. The order
 * of the arguments is fixed. If the String Array is null, the default
 * values will be used.
 *
 * @param args - The Java API arguments
 */
public void init(String[] args) {
    adminAPI = new AdminAPI();

    if (args != null && args.length == 4) {
        if (args[0] != null) {
            passwordAuthorityServerKeyStore = args[0];
        }
        if (args[1] != null) {
            passwordAuthorityUserName = args[0];
        }
        if (args[2] != null) {
            passwordAuthorityUserPassword = args[0];
        }
    }
}

```

```
        }
        if (args[3] != null) {
            passwordAuthorityServerHostName = args[0];
        }
    }
    adminAPI.login(passwordAuthorityServerKeyStore,
        passwordAuthorityUserName, passwordAuthorityUserPassword,
        passwordAuthorityServerHostName );
}

/**
 * A helper method which runs all add, update, search, view and delete
 * example methods.
 *
 */
public void runJavaAPIExample() {
    //Add
    addTargetServer();
    addTargetApplication();
    addTargetAccount();
    addTargetAlias();
    addRequestServer();
    addRequestScript();
    addAuthorization();
    addTargetGroup();
    addRequestGroup();
    addFilter();
    addRole();
    addUserGroup();
    addUser();
    addPasswordPolicy();
    addPasswordViewPolicy();

    //Update
    updateUserGroup();
    updateAgent();

    //Search
    searchRequestServer();

    //View Target Account Password
    viewTargetAccountPassword();

    //Delete
    deletePasswordViewPolicy();
    deletePasswordPolicy();
    deleteUser();
    deleteUserGroup();
    deleteRole();
    deleteRequestGroup();
    deleteTargetGroup();
    deleteAuthorization();
    deleteTargetAlias();
}
```

```
        deleteTargetServer();
        deleteRequestScript();
        deleteRequestServer();
    }

    /**
     * Logs out of the Password Authority Server.
     */
    public void logout() {
        adminAPI.logout();
    }

    /**
     * Adds a Target Server.
     */
    public void addTargetServer() {
        //Create a TargetServer instance by using AdminAPIFactory
        targetServer = AdminAPIFactory.createTargetServer();
        targetServer.setHostName(TARGET_SERVER_HOST_NAME);
        //Use the add method to create a Target Server
        result = adminAPI.add(targetServer);
        System.out.println("addTargetServer: " + result.getStatusMessage());
        //Retrieves a target server object from the result of the add command.
        targetServer = result.getValueAsTargetServer();

        //Prints the newly added Target server data.
        System.out.println("Target Server ID: " + targetServer.getID());
        System.out.println("Target Server host name: " +
            targetServer.getHostName());
        System.out.println("Target Server IP Address: " +
            targetServer.getIPAddress());
    }

    /**
     * Adds a Target Application.
     */
    public void addTargetApplication() {
        //Create a Unix TargetApplication instance by using AdminAPIFactory
        targetApplication = AdminAPIFactory.createTargetApplication();
        targetApplication.setTargetServerID(targetServer.getID());
        targetApplication.setName(TARGET_APPLICATION_NAME);
        targetApplication.setType(TARGET_APPLICATION_TYPE);
        targetApplication.setExtendedAttribute(SSH_PORT_ATTRIBUTE,
            SSH_PORT);
        result = adminAPI.add(targetApplication);
        System.out.println("addTargetApplication: " + result.getStatusMessage());
        targetApplication = result.getValueAsTargetApplication();
    }

    /**
     * Adds a Target Account.
     */
```

```

public void addTargetAccount() {
    //Create a TargetAccount instance by using AdminAPIFactory
    targetAccount = AdminAPIFactory.createTargetAccount();
    targetAccount.setTargetApplicationID(targetApplication.getID());
    targetAccount.setUserName(TARGET_ACCOUNT_USER_NAME);
    targetAccount.setPassword(TARGET_ACCOUNT_USER_PASSWORD);
    targetAccount.setPrivileged(false);
    //change setSynchronize to true if the Target Account is
    //to be synchronized.
    targetAccount.setSynchronize(false);
    targetAccount.setExtendedAttribute(USE_OTHER_ACCOUNT_TO_CHANGE_PASSWORD_ATTRIBUTE,
        String.valueOf(false));
    result = adminAPI.add(targetAccount);
    System.out.println("addTargetAccount: "+ result.getStatusMessage());
    targetAccount = result.getValueAsTargetAccount();
}

/**
 * Adds a Target Alias.
 */
public void addTargetAlias() {
    //Create a TargetAlias instance by using AdminAPIFactory
    targetAlias = AdminAPIFactory.createTargetAlias();
    targetAlias.setAccountID(targetAccount.getID());
    targetAlias.setName(TARGET_ALIAS_NAME);
    result = adminAPI.add(targetAlias);
    System.out.println("addTargetAlias: "+ result.getStatusMessage());
    targetAlias = result.getValueAsTargetAlias();
}

/**
 * Adds a Request Server.
 */
public void addRequestServer() {
    //Create a RequestServer instance by using AdminAPIFactory
    requestServer = AdminAPIFactory.createRequestServer();
    requestServer.setHostName(REQUEST_SERVER_HOST_NAME);
    result = adminAPI.add(requestServer);
    System.out.println("addRequestServer: "+ result.getStatusMessage());
    requestServer = result.getValueAsRequestServer();
}

/**
 * Adds a Request Script.
 */
public void addRequestScript() {
    //Create a RequestScript instance by using AdminAPIFactory
    requestScript = AdminAPIFactory.createRequestScript();
    requestScript.setRequestServerID(requestServer.getID());
    requestScript.setName(REQUEST_SCRIPT_NAME);
    requestScript.setExecutionPath(REQUEST_SCRIPT_EXECUTION_PATH);
    requestScript.setFilePath(REQUEST_SCRIPT_FILE_PATH);
    requestScript.setType(REQUEST_SCRIPT_TYPE);
}

```

```
        result = adminAPI.add(requestScript);
        System.out.println("addRequestScript: "+ result.getStatusMessage());
        requestScript = result.getValueAsRequestScript();
    }

    /**
     * Adds an Authorization.
     */
    public void addAuthorization() {
        //Create an Authorization instance by using AdminAPIFactory
        authorization = AdminAPIFactory.createAuthorization();
        authorization.setRequestServerID(requestServer.getID());
        authorization.setScriptID(requestScript.getID());
        authorization.setTargetAliasID(targetAlias.getID());
        result = adminAPI.add(authorization);
        System.out.println("addAuthorization: "+ result.getStatusMessage());
        authorization = result.getValueAsAuthorization();
    }

    /**
     * Adds a Target Group.
     */
    public void addTargetGroup() {
        //Create a Target Group instance by using AdminAPIFactory
        targetGroup = AdminAPIFactory.createGroup();
        targetGroup.setName(TARGET_GROUP_NAME);
        targetGroup.setType(Group.TYPE_TARGET);
        result = adminAPI.add(targetGroup);
        System.out.println("addTargetGroup: "+ result.getStatusMessage());
        targetGroup = result.getValueAsGroup();
    }

    /**
     * Adds a Request Group.
     */
    public void addRequestGroup() {
        //Create a Request Group instance by using AdminAPIFactory
        requestGroup = AdminAPIFactory.createGroup();
        requestGroup.setName(REQUEST_GROUP_NAME);
        requestGroup.setType(Group.TYPE_REQUESTOR);
        result = adminAPI.add(requestGroup);
        System.out.println("addRequestGroup: "+ result.getStatusMessage());
        requestGroup = result.getValueAsGroup();
    }

    /**
     * Adds a Filter to an existing Group.
     */
    public void addFilter() {
        //A filter can only be added to an existing group.
        Filter filter = AdminAPIFactory.createFilter();
        //Set the group id to the id of an existing group object.
        filter.setGroupID(requestGroup.getID());
    }
}
```

```

        //AttributeName is the field on which to create the filter.
        filter.setAttributeName(RequestServer.BEAN_PROPERTY_HOSTNAME);
        filter.setType(Filter.TYPE_CONTAINS);
        //The object class id can be set to the CLASS_ID of any of the supported
        //objects.
        filter.setObjectClassID(RequestServer.CLASS_ID);
        filter.setExpression(FILTER_EXPRESSION);
        result = adminAPI.add(filter);
        System.out.println("addFilter: "+ result.getStatusMessage());
        filter = result.getValueAsFilter();
    }

    /**
     * Adds a Role with add, update and delete Request Server permissions.
     */
    public void addRole() {
        //Create a Role instance by using AdminAPIFactory
        role = AdminAPIFactory.createRole();
        role.setName(ROLE_NAME);
        role.addPermission(ROLE_ADD_REQUEST_SERVER);
        role.addPermission(ROLE_UPDATE_REQUEST_SERVER);
        role.addPermission(ROLE_DELETE_REQUEST_SERVER);
        result = adminAPI.add(role);
        System.out.println("addRole: "+ result.getStatusMessage());
        role = result.getValueAsRole();
    }

    /**
     * Adds a User Group.
     */
    public void addUserGroup() {
        ArrayList newGroups = new ArrayList();

        //Create a UserGroup instance by using AdminAPIFactory
        userGroup = AdminAPIFactory.createUserGroup();
        userGroup.setName(USER_GROUP_NAME);
        //Create an ArrayList of the Group IDs that are to be added to the
        //UserGroup.
        newGroups.add(requestGroup.getID());
        newGroups.add(targetGroup.getID());
        userGroup.setGroupIDs(newGroups);
        userGroup.setRoleID(role.getID());
        result = adminAPI.add(userGroup);
        System.out.println("addUserGroup: "+ result.getStatusMessage());
        userGroup = result.getValueAsUserGroup();
    }

    /**
     * Adds a Password Authority User.
     */
    public void addUser() {
        ArrayList userGroupIDs = new ArrayList();

```

```

        //Create a User instance by using AdminAPIFactory
        user = AdminAPIFactory.createUser();
        user.setUserID(USER_USER_NAME);
        user.setPassword(USER_USER_PASSWORD);
        //Create an ArrayList of UserGroup IDs that are to be added to the
        //User.
        userGroupIDs.add(userGroup.getID());
        user.setUserGroupIDs(userGroupIDs);
        result = adminAPI.add(user);
        System.out.println("addUser: " + result.getStatusMessage());
        user = result.getValueAsUser();
    }

    /**
     * Adds a Password Composition Policy
     */
    public void addPasswordPolicy() {
        //Create a PasswordPolicy instance by using AdminAPIFactory
        passwordPolicy = AdminAPIFactory.createPasswordPolicy();
        passwordPolicy.setName(PASSWORD_POLICY_NAME);
        passwordPolicy.setDescription(PASSWORD_POLICY_DESCRIPTION);
        passwordPolicy.setExtendedAttribute(PasswordPolicy.MIN_LENGTH,
            String.valueOf(MINIMUM_PASSWORD_LENGTH));
        passwordPolicy.setExtendedAttribute(PasswordPolicy.MAX_LENGTH,
            String.valueOf(MAXIMUM_PASSWORD_LENGTH));
        passwordPolicy.setExtendedAttribute(PasswordPolicy.USE_ALPHA,
            String.valueOf(true));
        result = adminAPI.add(passwordPolicy);
        System.out.println("addPasswordPolicy: " + result.getStatusMessage());
        passwordPolicy = result.getValueAsPasswordPolicy();
    }

    /**
     * Adds a Password View Policy
     */
    public void addPasswordViewPolicy() {
        //Create a PasswordViewPolicy instance by using AdminAPIFactory
        passwordViewPolicy = AdminAPIFactory.createPasswordViewPolicy();
        passwordViewPolicy.setName(PASSWORD_VIEW_POLICY_NAME);
        passwordViewPolicy.setChangePasswordOnView(true);
        result = adminAPI.add(passwordViewPolicy);
        System.out.println("addPasswordViewPolicy: " +
            result.getStatusMessage());
        passwordViewPolicy = result.getValueAsPasswordViewPolicy();
    }

    /**
     * Updates an existing User Group.
     */
    public void updateUserGroup() {
        //An update uses an object retrieved via a search command or
        //the output of a previous add or update.
        userGroup.setDescription(USER_GROUP_DESCRIPTION);
    }

```



```

        result = adminAPI.update(userGroup);
        System.out.println("updateUserGroup: " + result.getStatusMessage());
        userGroup = result.getValueAsUserGroup();
        System.out.println("updateUserGroup description: " +
            userGroup.getDescription());
    }

    /**
     * Updates an Agent.
     */
    public void updateAgent() {
        //Create an Agent instance by using AdminAPIFactory
        agent = AdminAPIFactory.createAgent();
        agent.setID(AGENT_ID);
        agent.setHostName(AGENT_HOST_NAME);
        agent.setDeviceName(AGENT_DEVICE_NAME);
        agent.setActive(true);
        agent.setPreserveHostName(false);

        Attribute descriptor1 = AdminAPIFactory.createAttribute();
        descriptor1.setName("descriptor1");
        descriptor1.setValue(AGENT_DESCRIPTOR1);
        agent.setAttribute(descriptor1);

        Attribute descriptor2 = AdminAPIFactory.createAttribute();
        descriptor2.setName("descriptor2");
        descriptor2.setValue(AGENT_DESCRIPTOR2);
        agent.setAttribute(descriptor2);

        result = adminAPI.update(agent);
        System.out.println("addAgent: " + result.getStatusMessage());
        //Retrieves an agent object from the result of the add command.
        agent = result.getValueAsAgent();

        //Print the newly added Agent data.
        System.out.println("Agent ID : " + agent.getID());
        System.out.println("Agent Host Name : " + agent.getHostName());
        System.out.println("Agent Device Name : " + agent.getDeviceName());
        System.out.println("Agent Activation status : " + agent.isActive());
        System.out.println("Agent Descriptor1 : " + agent.getExtendedAttributeValue("descriptor1"));
        System.out.println("Agent Descriptor2 : " + agent.getExtendedAttributeValue("descriptor2"));
        System.out.println("Agent Preserve Host Name : " + agent.isPreserveHostName());
    }

    /**
     * Searches for a Request Server host name.
     *
     * If a parameter is specified, all matching Request Servers are
     * returned. If no parameter is specified, all Request Servers are
     * returned.
     */
    public void searchRequestServer() {
        RequestServer searchRequestServer;

```

```

List resultList;

//To search, a Request object must be created and passed to the
//AdminAPI execute method.
request = new Request();
request.setCommand(AdminAPICommandNames.SEARCH_REQUEST_SERVER);
request.setParameter(
    AdminAPIParameterNames.SEARCH_REQUEST_SERVER_HOST_NAME,
    REQUEST_SERVER_HOST_NAME);
result = adminAPI.execute(request);
System.out.println("searchRequestServer: "+ result.getStatusMessage());
//The search commands return a List object containing the result of
//your search.
resultList = result.getValueAsList(RequestServer.CLASS_ID);

if (resultList.size() > 0) {
    searchRequestServer = (RequestServer) resultList.get(0);
    System.out.println("searchRequestServer host name: " +
        searchRequestServer.getHostName());
}
}

/**
 * Views a Target Account Password. The result depends on the Password
 * View Policy of the Target Account.
 */
public void viewTargetAccountPassword() {
    TargetAccount viewPasswordAccount;
    //To view a password, a Request object must be created and passed to
    //the AdminAPI execute method.
    request = new Request();
    request.setCommand(AdminAPICommandNames.VIEW_ACCOUNT_PASSWORD);
    request.setParameter(
        AdminAPIParameterNames.VIEW_ACCOUNT_PASSWORD_TARGET_ACCOUNT_ID,
        targetAccount.getID());
    request.setParameter(
        AdminAPIParameterNames.VIEW_ACCOUNT_PASSWORD_ADMIN_USER_ID,
        VIEW_TARGET_ACCOUNT_USER_NAME);
    request.setParameter(
        AdminAPIParameterNames.VIEW_ACCOUNT_PASSWORD_ADMIN_PASSWORD,
        VIEW_TARGET_ACCOUNT_USER_PASSWORD);
    request.setParameter(
        AdminAPIParameterNames.VIEW_ACCOUNT_PASSWORD_REASON,
        VIEW_TARGET_ACCOUNT_REASON);
    result = adminAPI.execute(request);
    System.out.println("viewTargetAccountPassword: "+
        result.getStatusMessage());
    if (result.getWarningMessage() != null &&
        result.getWarningMessage().length() > 0) {
        System.out.println("viewTargetAccountPassword: " +
            result.getWarningMessage());
    }
    viewPasswordAccount = result.getValueAsTargetAccount();
}

```

```
        System.out.println("viewTargetAccountPassword password:" +
                           viewPasswordAccount.getPassword());
    }

    /**
     * Deletes an existing Password View Policy.
     */
    public void deletePasswordViewPolicy() {
        //Delete a PasswordViewPolicy
        result = adminAPI.delete(passwordViewPolicy);
        //The delete method will return the deleted object for future reference.
        passwordViewPolicy = result.getValueAsPasswordViewPolicy();
        System.out.println("deletePasswordViewPolicy: " +
                           result.getStatusMessage());
    }

    /**
     * Deletes a Password Composition Policy.
     */
    public void deletePasswordPolicy() {
        //Delete a PasswordPolicy
        result = adminAPI.delete(passwordPolicy);
        System.out.println("deletePasswordPolicy: "+ result.getStatusMessage());
    }

    /**
     * Deletes a Password Authority user.
     */
    public void deleteUser() {
        result = adminAPI.delete(user);
        System.out.println("deleteUser: "+ result.getStatusMessage());
    }

    /**
     * Deletes a Role.
     */
    public void deleteRole() {
        result = adminAPI.delete(role);
        System.out.println("deleteRole: "+ result.getStatusMessage());
    }

    /**
     * Deletes a User Group.
     */
    public void deleteUserGroup() {
        result = adminAPI.delete(userGroup);
        System.out.println("deleteUserGroup: "+ result.getStatusMessage());
    }

    /**
     * Deletes a Request Group.
     */
    public void deleteRequestGroup() {
```

```
//Delete a Group
result = adminAPI.delete(requestGroup);
System.out.println("deleteRequestGroup: "+ result.getStatusMessage());
}

/**
 * Deletes a Target Group.
 */
public void deleteTargetGroup() {
    //Delete a Group
    result = adminAPI.delete(targetGroup);
    System.out.println("deleteTargetGroup: "+ result.getStatusMessage());
}

/**
 * Deletes an Authorization.
 */
public void deleteAuthorization() {
    //Delete the Authorization
    result = adminAPI.delete(authorization);
    System.out.println("deleteAuthorization: "+ result.getStatusMessage());
}

/**
 * Deletes a Target Alias.
 */
public void deleteTargetAlias() {
    //Delete the Target Alias
    result = adminAPI.delete(targetAlias);
    System.out.println("deleteTargetAlias: "+ result.getStatusMessage());
}

/**
 * Deletes a Target Server. Deleting a Target Server will also delete
 * all associated Target Applications and Target Accounts.
 */
public void deleteTargetServer() {
    //Delete the Target Server
    result = adminAPI.delete(targetServer);
    System.out.println("deleteTargetServer: "+ result.getStatusMessage());
}

/**
 * Deletes a Request Script.
 */
public void deleteRequestScript() {
    //Delete the Request Script
    result = adminAPI.delete(requestScript);
    System.out.println("deleteRequestScript: "+ result.getStatusMessage());
}

/**
 * Deletes a Request Server.
 */
```

```

    */
    public void deleteRequestServer() {
        //Delete the Request Server
        result = adminAPI.delete(requestServer);
        System.out.println("deleteRequestServer: "+ result.getStatusMessage());
    }
}

```

## Use the Remote CLI

After the Remote CLI is set up, you can execute a command or scripts of commands to administer Credential Manager or Secrets Management functions. This content in this section explains how to execute these commands.

**Use the table of contents to access the topics in this section.**

Also see the following topics for a list of CLI commands available for each CLI:

- [Credential Manager CLI Commands](#)
- [Secrets Management CLI Commands](#)

## Remote CLI Command Syntax

UNIX/Linux and Windows platforms support the CLI. To authenticate with the CLI and run a command, use the following syntax:

```

capam_command capam=hostname adminUserID=user_name [adminPassword=password]
cmdName=command [<parameter>=<value>]

```

### NOTE

SAML users are not supported for Remote CLI authentication.

The commands a user can execute are determined by the roles that are assigned to that user. See [Add or Modify Credential Manager Roles](#), or [About Secrets Management and Roles](#), as appropriate.

On UNIX, traditional and GNU style aliases for some parameters exist:

- `capam=hostname` can also be specified as `-n <hostname>`

### NOTE

If you run a command that requires an IPv6 address, you must enclose the address in square brackets. For example:

```
capam=[fd6d:8d64:af0c:1:0:252: 44:114]
```

- `adminUserID=user_name` can also be specified as `-u user_name` or `--adminUserID=user_name`
- `adminPassword=password` can also be specified as `-p password` or `--adminPassword=password`

If you do not specify the password as an option, you are prompted for it before the command is processed.

### TIP

- The CLI often requires commands that are long. To allow commands to span multiple lines in UNIX, use the continuation character, which is a backslash (\).
- If a parameter value contains a space, enclose the entire value pair definition in quotes. For example, enter "[TargetApplication.name](#)=AWS Access Credential Accounts" rather than [TargetApplication.name](#)="AWS Access Credential Accounts".

## Execute Commands Individually or as a Batch Sequence

The CLI can process commands individually or as a batch sequence. In both cases, the commands and argument values are the same.

Due to restrictions in the number of arguments that the Windows batch utility permits, you cannot run all commands individually. To work around this limitation, use the `batchSequence` command. For more information about the `batchSequence` command, see [Batch CLI Command Execution](#).

## Remote CLI Return Values

The CLI returns an XML string for each command. The return string includes the following information:

- a status code
- a status description
- a result with every parameter that is associated with the command object. The following XML structure is an example:

```
<CommandResult>
  <cr.itemNumber>0</cr.itemNumber>
  <cr.statusCode>400</cr.statusCode>
  <cr.statusDescription>Success.</cr.statusDescription>
</CommandResult>
```

For improved readability of the output, direct the XML structure to a separate file and then open it with an XML editor.

## Command Example

This example shows the **getErrorCodes** command. This command takes no parameters. The command returns an XML structure listing each Credential Manager server error code and its description. The command also directs the output of the `getErrorCodes` CLI command to a file named `error_codes.xml`.

### Follow these steps:

1. Use the following command:

```
capam_command capam=hostname -u admin -p password capam=mycompany.com
cmdName=getErrorCodes > error_codes.xml
```

Where *password* is the password of the admin account  
Credential Manager produces an XML command string to the `error_codes.xml` file.

2. Open the `error_codes.xml` file with an XML editor, such as Notepad++.

## Batch CLI Command Execution

The **batchSequence** CLI command enables the execution of multiple CLI commands in a single transaction. The CLI commands are specified as a sequence of XML elements in an XML-formatted file. Batch processing is primarily intended for a batch import of data, such as adding many target accounts to Credential Manager or many secret users to Secrets Management. You can use batch processing more generally. You can also use batch processing as an interface between automated system and the CLI.

## Batch Command Example

### Follow these steps:

1. Create a batch processing XML file to use as input for the `batchSequence` command. Use the XML schema in [Remote CLI XML Schema for Batch Processing](#) to ensure that the file is well formatted.

For example, the following file is named `AddAll.xml`. The file encloses a CLI request specifying two Credential Manager commands and their arguments (CLI requests for Secrets Management are structured identically). The two commands add a target application and a target account within that application:

```
<?xml version="1.0" encoding="UTF-8"?>
<CLI_REQUEST
  xmlns="http://www.cloakware.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.cloakware.com/opt/cloakware/cspmserver/tools/cli/cspmcli.xsd">
  <COMMAND name="addTargetServer">
    <COMMAND_PARAMETERS>
      <PARAMETER>
        <NAME>TargetServer.hostName</NAME>
        <VALUE>Ottawa-Lab3.cloakware.com</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>TargetServer.ipAddress</NAME>
        <VALUE>10.5.0.3</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>Attribute.descriptor1</NAME>
        <VALUE>Ottawa</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>Attribute.descriptor2</NAME>
        <VALUE>Lab</VALUE>
      </PARAMETER>
    </COMMAND_PARAMETERS>
  </COMMAND>

  <COMMAND name="addTargetApplication">
    <COMMAND_PARAMETERS>
      <PARAMETER>
        <NAME>TargetServer.hostName</NAME>
        <VALUE>Ottawa-Lab3.cloakware.com</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>TargetApplication.type</NAME>
        <VALUE>Generic</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>TargetApplication.name</NAME>
        <VALUE>Generic account type</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>Attribute.descriptor1</NAME>
        <VALUE>Ottawa</VALUE>
      </PARAMETER>
      <PARAMETER>
        <NAME>Attribute.descriptor2</NAME>
        <VALUE>Lab</VALUE>
      </PARAMETER>
    </COMMAND_PARAMETERS>
  </COMMAND>
```

```
</CLI_REQUEST>
```

## 2. Run the batch processing command with your file as input.

```
capam_command capam=pam02.ca.com adminUserID=admin cmdName=batchSequence inputfile=AddAll.xml
outputfile=results.xml
```

## 3. Enter your password at the prompt. After a brief moment of processing, Credential Manager presents the batch results as follows:

```
<BatchCommandResult>
  <CommandResult>
    <cr.itemNumber>0</cr.itemNumber>
    <cr.commandName>addTargetServer</cr.commandName>
    <cr.statusCode>400</cr.statusCode>
    <cr.statusDescription>Success</cr.statusDescription>
    <cr.result>
      <TargetServer>
        <Attribute.descriptor2>Lab</Attribute.descriptor2>
        <Attribute.descriptor1>Ottawa</Attribute.descriptor1>
        <ID>3</ID>
        <createDate>Mon Nov 12 17:18:41 EST 2007</createDate>
        <updateDate>Mon Nov 12 17:18:41 EST 2007</updateDate>
        <createUser>admin</createUser>
        <updateUser>admin</updateUser>
        <hash>qn/wPB8BBtxfu7/cJMKc3Bn+vCE=</hash>
        <hostName>Ottawa-Lab3.cloakware.com</hostName>
        <IPAddress>10.5.0.3</IPAddress>
      </TargetServer>
    </cr.result>
  </CommandResult>

  <CommandResult>
    <cr.itemNumber>1</cr.itemNumber>
    <cr.commandName>addTargetApplication</cr.commandName>
    <cr.statusCode>400</cr.statusCode>
    <cr.statusDescription>Success</cr.statusDescription>
    <cr.result>
      <TargetApplication>
        <Attribute.descriptor2>Lab</Attribute.descriptor2>
        <Attribute.descriptor1>Ottawa</Attribute.descriptor1>
        <ID>3</ID>
        <createDate>Mon Nov 12 17:18:41 EST 2007</createDate>
        <updateDate>Mon Nov 12 17:18:41 EST 2007</updateDate>
        <createUser>admin</createUser>
        <updateUser>admin</updateUser>
        <hash>I8XvBL6zIT/mCaDwy/F58Q2Z9LI=</hash>
        <targetServerID>3</targetServerID>
        <type>Generic</type>
        <name>Generic account type</name>
        <policyID>0</policyID>
      </TargetApplication>
    </cr.result>
  </CommandResult>
</BatchCommandResult>
```



## Remote CLI XML Schema for Batch Processing

Use the Remote CLI XML schema for batch processing to ensure that your input file is appropriately formatted.

```
<?xml version="1.0" encoding="utf-8" ?>

<xs:schema      xmlns="http://www.cloakware.com"
                 xmlns:xs="http://www.w3.org/2001/XMLSchema"
                 targetNamespace="http://www.cloakware.com"
                 elementFormDefault="qualified">
  <xs:element name="PARAMETER">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="NAME" type="xs:string"
                     minOccurs="1" maxOccurs="1"/>
        <xs:element name="VALUE" type="xs:string"
                     minOccurs="1" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="COMMAND_PARAMETERS">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="PARAMETER" minOccurs="1"
                     maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="COMMAND">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="COMMAND_PARAMETERS"
                     minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
      <xs:attribute name="name" type="xs:string" use="required" />
    </xs:complexType>
  </xs:element>

  <xs:element name="CLI_REQUEST" >
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="COMMAND" minOccurs="1"
                     maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

## Credential Manager CLI Commands

You can use the Remote CLI to control and configure Credential Manager. This command-line interface allows administrators to provide scripted functionality to complete management and integration tasks. The Remote CLI supports a limited subset of features that are available through the GUI. There are also some commands that are only available through the CLI.

### NOTE

String searches in CLI commands are case sensitive. That is, a search for `deviceName=server` returns "server1" and "server2", but not "Server3."

Use the table of contents to access the command descriptions.

### addAuthorization

Use the `addAuthorization` command to add an authorization mapping. This gives a requesting application, request server, or request group permission to query credentials for a target alias or target group. The Windows CLI allows up to nine parameters, including the mandatory `adminUserID` and `capam`. To enter the `addAuthorization` command with more than nine parameters, use the `batchSequence` command with an XML formatted input file.

#### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=addAuthorization
RequestServer.hostName=myhostname.mydomain.com

RequestScript.name=example.pl RequestScript.executionPath=/usr/tmp/examples
Authorization.checkExecutionID=true

Authorization.executionUser=auser Authorization.checkPath=true
TargetAlias.name=myaliasname Authorization.checkScriptHash=true
```

### Parameters

#### TargetAlias.name

Specifies the target alias name.

Required	Default Value	Valid Values
One of <code>TargetAlias.name</code> , <code>TargetAlias.ID</code> , <code>Authorization.targetGroupName</code> , or <code>Authorization.targetGroupId</code> is required.	N/A	This value must match the target alias name that is registered in Credential Manager.

#### TargetAlias.ID

Specifies the target alias ID.

Required	Default Value	Valid Values
One of <code>TargetAlias.name</code> , <code>TargetAlias.ID</code> , <code>Authorization.targetGroupName</code> , or <code>Authorization.targetGroupId</code> is required.	N/A	Use <code>searchTargetAlias</code> to retrieve the <code>TargetAlias.ID</code> .

**Authorization.targetGroupName**

Specifies the target group name.

Required	Default Value	Valid Values
One of TargetAlias.name, TargetAlias.ID, Authorization.targetGroupName, or Authorization.targetGroupId is required.	N/A	This value must match the target group name that is registered in Credential Manager.

**Authorization.targetGroupId**

Specifies the target group ID.

Required	Default Value	Valid Values
One of TargetAlias.name, TargetAlias.ID, Authorization.targetGroupName, or Authorization.targetGroupId is required.	N/A	Numeric.

**RequestServer.hostName**

Specifies the request server host name on which the requesting application resides.

Required	Default Value	Valid Values
One of RequestServer.hostName, RequestServer.ID, Authorization.requestGroupName, or Authorization.requestGroupId is required.	N/A	This value must match the request server name that is registered in Credential Manager.

**RequestServer.ID**

Specifies the request server ID on which the requesting application resides.

Required	Default Value	Valid Values
One of RequestServer.hostName, RequestServer.ID, Authorization.requestGroupName, or Authorization.requestGroupId is required.	N/A	Use searchRequestServer to retrieve the RequestServer.ID.

**Authorization.requestGroupName**

Specifies the request group name the requesting application is a member of resides.

Required	Default Value	Valid Values
One of RequestServer.hostName, RequestServer.ID, Authorization.requestGroupName, or Authorization.requestGroupId is required.	N/A	This value must match the request group name that is registered in Credential Manager.

**Authorization.requestGroupId**

Specifies the request group name the requesting application is a member of resides.

Required	Default Value	Valid Values
One of RequestServer.hostName, RequestServer.ID, Authorization.requestGroupName, or Authorization.requestGroupId is required.	N/A	Numeric.

### **RequestScript.name**

Specifies the requesting application name.

Required	Default Value	Valid Values
One of RequestScript.name or RequestScript.ID is required.	N/A	This value must match the script name that is registered in Credential Manager.

### **RequestScript.ID**

Specifies the requesting application ID. Set this value to -1 to specify All request scripts for the indicated request server. Setting this to -1 also sets Authorization.checkPath, Authorization.checkFilePath, and Authorization.checkScriptHash to false.

Required	Default Value	Valid Values
yes	N/A	-1 or use searchRequestScript to retrieve the RequestScript.ID.

### **RequestScript.executionPath**

Specifies the requesting application execution path, as registered in Credential Manager.

Required	Default Value	Valid Values
Required if RequestScript.name is used.	N/A	This value must match the script execution path that is registered in Credential Manager.

### **Authorization.checkExecutionID**

Set Authorization.checkExecutionID=true to indicate that the execution user ID be validated.

Required	Default Value	Valid Values
no	false	true, false

### **Authorization.executionUser**

A comma-delimited list of execution user IDs. The IDs are only validated if Authorization.checkExecutionID=true.

Required	Default Value	Valid Values
no	N/A	String.

### **Authorization.checkPath**

Set Authorization.checkPath=true to indicate that the script execution path be validated.

Required	Default Value	Valid Values
no	false	true, false

### **Authorization.checkFilePath**

Set Authorization.checkFilePath=true to indicate that the script file path be validated.

Required	Default Value	Valid Values
no	false	true, false

### **Authorization.checkScriptHash**

Set Authorization.checkScriptHash=true to indicate that script hash integrity verification be performed.

Required	Default Value	Valid Values
no	false	true, false

## **addFilter**

Use the addFilter command to add a filter to a target group or request group. The group must first be added using the addGroup command.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addFilter Group.ID=3
  Filter.objectClassId=c.cw.m.ts

  Filter.attribute=hostName Filter.type=contains Filter.expression="mydomain"
```

## **Parameters**

### **Group.ID**

Specifies the ID of the request or target group. It must be an integer greater than or equal to 1.

Required	Default Value	Valid Values
yes	N/A	Integer

### **Filter.objectClassId**

Specifies the type of object to filter. Class IDs are specific to group type.

Required	Default Value	Valid Values
yes	N/A	c.cw.m.ts, c.cw.m.tp, c.cw.m.ac, c.cw.m.rs, c.cw.m.sc

### **Filter.attribute**

Specifies the filter attribute. If static, attribute must be ID. If dynamic, attributes are specific to objectClassId.

Required	Default Value	Valid Values
yes	N/A	String.

### **Filter.type**

Specifies the filter type. If group is static, only equals is valid.

Required	Default Value	Valid Values
yes	N/A	equals, beginswith, contains, endswith, notcontains

### **Filter.expression**

Specifies the filter expression. If group is static, expression can only be an integer greater than or equal to 1.

Required	Default Value	Valid Values
yes	N/A	String, Integer

## **addGroup**

Use the addGroup command to add either a target or request group to Privileged Access Manager. Use the addFilter command to add filters to the group.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addGroup
  Group.name=TokyoTargets Group.description="Targets in Tokyo" Group.type=target
```

## **Parameters**

### **Group.name**

Specifies the name of the target or request group.

Required	Default Value	Valid Values
yes	N/A	String

### **Group.description**

Specifies the description of the group.

Required	Default Value	Valid Values
no	N/A	String

### **Group.type**

Set Group.type=requestor for Request groups. Set Group.type=target for Target groups.

Required	Default Value	Valid Values
yes	N/A	requestor, target

### **Group.dynamic**

Set Group.dynamic=true for dynamic Request/Target groups, false for static Request/Target groups.

Required	Default Value	Valid Values
no	true	true, false

### **Group.permissions**

ArrayList object of filters, or XML encoded ArrayList of filters. If not set, the filters are cleared.

Required	Default Value	Valid Values
no	N/A	XML

Required	Default Value	Valid Values
yes	N/A	String, Integer

## **addPasswordPolicy**

Use the addPasswordPolicy command to add a Password Composition Policy in Privileged Access Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addPasswordPolicy
  PasswordPolicy.name=passwordPolicyName

Attribute.composedOfUpperCaseCharacters=true
Attribute.firstCharacterUpperCase=true
```

### **Parameters**

#### **PasswordPolicy.name**

The name of the password policy.

Required	Default Value	Valid Values
Yes	None	String

#### **PasswordPolicy.description**

The description of the password policy.

Required	Default Value	Valid Values
No	Blank	String

**Attribute.passwordPrefix**

The prefix for all passwords that are mandated by your password policy.

Required	Default Value	Valid Values
No	None	Constrained by your other settings.

**Attribute.composedOfUpperCaseCharacters**

Set to true to mandate that your password policy requires uppercase characters.

Required	Default Value	Valid Values
No	false	true, false

**Attribute.composedOfLowerCaseCharacters**

Set to true to mandate that your password policy requires lowercase characters.

Required	Default Value	Valid Values
No	false	true, false

**Attribute.composedOfNumericCharacters**

Set to true to mandate that your password policy requires numeric characters.

Required	Default Value	Valid Values
No	false	true, false

**Attribute.composedOfSpecialCharacters**

Set to true to mandate that your password policy requires special characters.

Required	Default Value	Valid Values
No	false	true, false

**Attribute.specialCharacters**

The list of all special characters that are allowed by your password policy.

Required	Default Value	Valid Values
No	None	!#\$%()*+,-./:;=?@[\\]^_`{ }~

**Attribute.firstCharacterUpperCase**

Set to true to mandate that your password policy requires the first character to be uppercase. If you select more than one first character requirement, they are combined. For example, if both Attribute.firstCharacterUpperCase and Attribute.firstCharacterLowerCase are true, then the policy requires the first character to be either upper or lowercase.

Required	Default Value	Valid Values
No	false	true, false

**Attribute.firstCharacterLowerCase**



Set to true to mandate that your password policy requires the first character to be lowercase. If you select more than one first character requirement, they are combined. For example, if both `Attribute.firstCharacterUpperCase` and `Attribute.firstCharacterLowerCase` are true, then the policy requires the first character to be either upper or lowercase.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.firstCharacterNumeric**

Set to true to mandate that your password policy requires the first character to be numeric. If you select more than one first character requirement, they are combined. For example, if both `Attribute.firstCharacterUpperCase` and `Attribute.firstCharacterNumeric` are true, then the policy requires the first character to be either uppercase or numeric.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.firstCharacterSpecial**

Set to true to mandate that your password policy requires the first character to be a special character. If you select more than one first character requirement, they are combined. For example, if both `Attribute.firstCharacterUpperCase` and `Attribute.firstCharacterSpecial` are true, then the policy requires the first character to be either uppercase or a special character.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.firstCharacterSpecials**

The list of all special characters that are allowed as a first character by your password policy.

Required	Default Value	Valid Values
No	None	!#\$%()*+,-./:;=?@[\\]^_`{ }~

#### **Attribute.mustNotContainConsecutiveDuplicateCharacters**

Set to true to mandate that your password policy does not allow any repeating characters.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.mustNotContainAnyDuplicateCharacters**

Set to true to mandate that your password policy does not allow any duplicate characters.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.mustNotContainCharacters**

Set to true to mandate that your password policy prohibits certain uppercase, lowercase, or numeric characters.

Required	Default Value	Valid Values
No	false	true, false

#### **Attribute.composedOfMustNotContainCharacters**

The list of all characters that your password policy does not allow. Do not prohibit characters that are allowed in other attributes.

Required	Default Value	Valid Values
No	Blank	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789

#### **Attribute.minLength**

Set the minimum length of characters to mandate by your password policy.

Required	Default Value	Valid Values
No	4	1– 2048

#### **Attribute.maxLength**

Set the maximum length of characters to mandate by your password policy.

Required	Default Value	Valid Values
No	16	1– 2048

#### **NOTE**

Although PAM supports a maximum password length of 2048 characters, target systems may have lower limits. For example, the maximum password length on a Linux system is 511 characters. Therefore, if you want PAM to manage accounts on a Linux system as synchronized accounts, set the Attribute.maxLength value to no more than 511.

#### **Attribute.minIterationsBeforeReuse**

Set the minimum number of iterations before a password can be reused.

Required	Default Value	Valid Values
No	0	Numeric

#### **Attribute.minDaysBeforeReuse**

Set the minimum number of days before a password can be reused.

Required	Default Value	Valid Values
No	0	Numeric

#### **Attribute.enableMaxPasswordAge**

Set to true to enable maximum password age in your password policy.

Required	Default Value	Valid Values
No	false	true, false

### **Attribute.maxPasswordAge**

Set the maximum password age in days. After this many days, passwords will have to be changed.

Required	Default Value	Valid Values
Yes, if Attribute.enableMaxPasswordAge is set to true.	None	Numeric

### **PasswordViewPolicy.passwordViewRequestBanner**

The banner description for the Password View Policy.

Required	Default Value	Valid Values
No	None	String

## **addPasswordViewPolicy**

Use the addPasswordViewPolicy command to add a password view policy to Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addPasswordViewPolicy
  PasswordViewPolicy.name=restrictedAccounts
```

```
PasswordViewPolicy.changePasswordOnView=true
PasswordViewPolicy.checkinCheckoutRequired=true
PasswordViewPolicy.checkinCheckoutInterval=240
```

## **Parameters**

### **PasswordViewPolicy.name**

The name of the password view policy.

Required	Default Value	Valid Values
yes	N/A	String

### **PasswordViewPolicy.description**

A description of the password view policy.

Required	Default Value	Valid Values
no	N/A	String

### **PasswordViewPolicy.changePasswordOnView**

Set this parameter to true to instruct Credential Manager to change the password after a password view request.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.changePasswordOnSso**

Set this parameter to true to instruct Credential Manager to change the password after a password SSO request is retrieved but not viewed.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.passwordChangeInterval**

If the changePasswordOnView parameter is set to true, this parameter determines the length of time (in minutes) before Credential Manager changes the password.

Required	Default Value	Valid Values
Must be specified if PasswordViewPolicy.changePasswordOnView is true.	60	Numeric value greater than 0

#### **PasswordViewPolicy.checkinCheckoutRequired**

Set this parameter to true to indicate that an account must be checked out before anyone can view the password. When checked out, the account password cannot be changed.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.checkinCheckoutInterval**

Determines the length of time (in minutes) an account can remain checked out before it is automatically checked back in by the system.

Required	Default Value	Valid Values
Specify if PasswordViewPolicy.checkinCheckoutRequired is true	60	Numeric value greater than 0

#### **PasswordViewPolicy.dualAuthorization**

Set PasswordViewPolicy.dualAuthorization=true to indicate that a request to view a password must be approved by another user before proceeding. Note that the XML content returned by PAM shows this parameter with the name **dualAuthorizationRequired**.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.dualAuthorizationInterval**

This parameter determines the default length of time (in minutes) a password view request remains active in the system.

Required	Default Value	Valid Values
Must be specified if PasswordViewPolicy.dualAuthorization is true.	60	Numeric value greater than 0

#### **PasswordViewPolicy.retrospectiveApprovalRequired**

Set PasswordViewPolicy.retrospectiveApprovalRequired=true to indicate that a request to view a password requires retrospective approval. (Access is granted immediately and specified approvers notified.)

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.approvers**

Lists the users who are authorized to approve or deny password requests for accounts that use this password policy.

Required	Default Value	Valid Values
If PasswordViewPolicy.dualAuthorization is set to true, set this parameter or the PasswordViewPolicy.approverIDs parameter	N/A	List of comma-separated usernames. Example: jbauer,mdessler,dpalmer

#### **PasswordViewPolicy.approverIDs**

The list of user IDs who are authorized to approve or deny password requests for accounts that use this password policy.

Required	Default Value	Valid Values
If PasswordViewPolicy.dualAuthorization is true, set this parameter or the PasswordViewPolicy.approvers parameter	Use searchUser to retrieve a list of user IDs	List of comma-separated user IDs. Example: 11,19,15

#### **PasswordViewPolicy.authenticationRequiredSso**

Set this parameter to true to indicate that the requesting user must provide their own password before using the account for auto-connect.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.authenticationRequired**

Set this parameter to true to indicate that the requesting user must provide their own password before viewing the account password.

Required	Default Value	Valid Values
no	true	true, false

#### **PasswordViewPolicy.enableOneClickApproval**

Set this parameter to true to enable one click dual authorization approval. When enabled, dual authorization emails include links that allow the approval of requests without requiring the approver to log into the system.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.PasswordViewRequestMaxInterval**

The maximum Interval between the start and end date of a dual authorization password view request.

Required	Default Value	Valid Values
no	60	Numeric value greater than 0.

#### **PasswordViewPolicy.PasswordViewRequestMaxDays**

The maximum number of days in the future that a password view request can be requested.

Required	Default Value	Valid Values
no	14	Numeric value greater than 0.

#### **PasswordViewPolicy.emailNotificationRequired**

This parameter sends an email notification when someone views a password. If you set this value to true, specify at least one entry for the PasswordViewPolicy.emailNotificationUsers or PasswordViewPolicy.emailNotificationUserIDs parameters. If both parameters have at least one entry, Credential Manager uses the PasswordViewPolicy.emailNotificationUsers list.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.emailNotificationToDualAuthApprovers**

This parameter sends an email notification only to dual authorization approvers. If you set this parameter to true, specify at least one entry in the PasswordViewPolicy.approvers list.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.emailNotificationUsers**

Lists users that receive email notifications when someone views a password. User names in the list must be separated by a comma.

Required	Default Value	Valid Values
no	N/A	user name

#### **PasswordViewPolicy.emailNotificationUserIDs**

Lists user IDs for users that receive email notifications when someone views a password. User names in the list must be separated by a comma.

Required	Default Value	Valid Values
no	N/A	user IDs

#### **PasswordViewPolicy.emailNotificationToActiveUsers**

This parameter sends an email notification to any active user when someone views a password.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.passwordViewRequestBanner**

The banner description for the Password View Policy.

Required	Default Value	Valid Values
no	None	Alphanumeric, -, . and space character

#### **NOTE**

For more information on the following parameters, see their UI equivalents in the [Create a Basic Password View Policy](#) topic.

#### **PasswordViewPolicy.reasonRequiredView**

If set to true, a dialog appears when a user tries to view an Account password. The user selects a Reason and enters a Description and Reference Code to view the password. Select the View Credential (eye icon) for an Account on the Account List page or on the Account Details page.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.reasonRequiredSso**

If set to true, a dialog appears when a user tries to auto-connect. The user selects a Reason and enters an optional Description and optional Reference Code to auto-connect.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.exclusiveCheckoutRequired**

If set to true, this option specifies that credentials are checked in if all connections are closed.

#### **NOTE**

If you select this option, all view properties and the Check-out/Check-in property are unavailable.

If PasswordViewPolicy.exclusiveCheckoutRequired is selected with service desk integration, the Reason Required for View option is selected but disabled. Even though it is selected, the functionality of view password

does not work, as exclusive checkout takes precedence. Viewing of a password is disabled when the account is associated with exclusive checkout on auto connect.

Required	Default Value	Valid Values
no	false	true, false

### **PasswordViewPolicy.changePasswordOnSessionEnd**

If set to true, all passwords that are used to log in to target servers are changed when the user session in Privileged Access Manager ends. The connection can end because the user logs out, a session times out, or connectivity is lost. This option does not apply to "View Password."

Required	Default Value	Valid Values
no	false	true, false

### **PasswordViewPolicy.changePasswordOnConnectionEnd**

If set to true, the password is automatically changed when the user's SSH or RDP connection to a target server ends. The connection can end because the connection times-out, the user terminates the connection, or the connection is lost. This option does not apply to "View Password."

Required	Default Value	Valid Values
no	false	true, false

## **addRequestScript**

Use the addRequestScript command to add a request application to Credential Manager.

### **Example**

```
capam_command capame=capamServer adminUserID=admin cmdName=addRequestScript
RequestServer.hostName=myhostname.mydomain.com
```

```
RequestScript.name=example.pl RequestScript.executionPath=/usr/tmp/examples
RequestScript.filePath=/usr/tmp/examples RequestScript.type=Perl
```

### **Parameters**

#### ***RequestServer.hostName***

The request server host name on which the requesting application resides.

Required	Default Value	Valid Values
One of RequestServer.hostName or RequestServer.ID is required.	N/A	This value must match the request server name that is registered in Credential Manager.

#### **RequestServer.ID**



The request server ID on which the requesting application resides.

Required	Default Value	Valid Values
One of RequestServer.hostName or RequestServer.ID is required.	N/A	Use searchRequestServer to retrieve the RequestServer.ID.

### **RequestScript.name**

The requesting application name.

Required	Default Value	Valid Values
yes	N/A	String.

### **RequestScript.executionPath**

The location from which the requesting application is executed.

Required	Default Value	Valid Values
yes	N/A	String.

### **RequestScript.filePath**

The location in which the requesting application resides.

Required	Default Value	Valid Values
no	N/A	String.

### **RequestScript.type**

The programming language in which the requesting application is written.

Required	Default Value	Valid Values
yes	N/A	C, C++, C#, csh, Java, ksh, Perl, ksh, VB, VB.NET, VC++, Other

### **Attribute.descriptor1**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

### **Attribute.descriptor2**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

## addRequestServer

Use the addRequestServer command to add a request server (Privileged Access Manager Credential Manager client) to Privileged Access Manager Credential Manager. CA Technologies recommends that you use the auto-discovery feature for adding request servers.

### Example

```
cspmserver_admin adminUserID=admin cmdName=addRequestServer
RequestServer.hostName=myhostname.mydomain.com RequestServer.active=true
RequestServer.autoPatch=true
```

### Parameters

#### RequestServer.hostName

The host name of the request server.

Required	Default Value	Valid Values
yes	N/A	String

#### RequestServer.deviceName

The device name of the request server.

Required	Default Value	Valid Values
no	Same as host name.	String

#### RequestServer.active

Set RequestServer.active=true to activate the request server. Set RequestServer.active=false to deactivate the request server.

Required	Default Value	Valid Values
no	false	true, false

#### RequestServer.autoPatch

Set RequestServer.autoPatch=true to indicate that patches should be applied automatically.

Required	Default Value	Valid Values
no	false	true, false

#### RequestServer.preserveHostName

Set RequestServer.preserveHostName=true to indicate that the request server host name should not be overwritten each time the client registers.

Required	Default Value	Valid Values
no	Determined by the value of system property setting "AppDefaultPreserveClientHostName".	true, false

### Attribute.descriptor1

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String

### **Attribute.descriptor2**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String

## **addRequestServerDefaults**

Use the addRequestServerDefaults command to add a request server defaults to Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=addRequestServerDefaults RequestServerDefaults.subnet=122.111.0.0/16

RequestServerDefaults.active=true RequestServerDefaults.type=CLIENT
RequestServerDefaults.descriptor1=awsApiProxy
```

### **Parameters**

#### **RequestServerDefaults.subnet**

The subnet filter to apply defaults to request servers.

Required	Default Value	Valid Values
yes	N/A	String

#### **RequestServerDefaults.type**

The type filter to apply defaults to request servers.

Required	Default Value	Valid Values
yes	N/A	CLIENT, AGENT, ALL

#### **RequestServerDefaults.active**

The default setting for RequestServer.active during auto-register.

Required	Default Value	Valid Values
yes	N/A	true, false

#### **RequestServerDefaults.descriptor1**

The default setting for Attribute.descriptor1 during auto-register.

Required	Default Value	Valid Values
no	N/A	String

### **RequestServerDefaults.descriptor2**

The default setting for Attribute.descriptor2 during auto-register.

Required	Default Value	Valid Values
no	N/A	String

## **addRole**

Use the addRole command to add a user role to Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addRole
  Role.name=myRole Role.description="Manages patches"

Role.permissions="activatePatch,
  addPatch,deletePatch,getPatchDetail,listPatch,updatePatch"
```

### **Parameters**

#### **Role.name**

The name of the role.

Required	Default Value	Valid Values
yes	N/A	String. A unique name in Credential Manager

#### **Role.description**

The description of the role.

Required	Default Value	Valid Values
no	N/A	String

#### **Role.permissions**

A comma-delimited list of permissions.

Required	Default Value	Valid Values
yes	N/A	String. See <a href="#">Add or Modify Credential Manager Roles</a> for a list of valid permissions.

## addSSHKeyPairPolicy

Use the addSSHKeyPairPolicy command to add an SSH Key Pair Policy to Privileged Access Manager.

### Example

```
capam_command capam=capamServer adminUserID=super adminPassword=password
cmdName=addSSHKeyPairPolicy
```

```
SSHKeyPairPolicy.name=Testing SSHKeyPairPolicy.keyType=RSA
SSHKeyPairPolicy.keyLength=2048
```

### Parameters

#### SSHKeyPairPolicy.name

The policy name.

Required	Default Value	Valid Values
Yes	N/A	A String

#### SSHKeyPairPolicy.description

The policy description.

Required	Default Value	Valid Values
No	N/A	A String

#### SSHKeyPairPolicy.keyType

The key type.

Required	Default Value	Valid Values
Yes	N/A	ECDSA or RSA or DSA

#### SSHKeyPairPolicy.keyLength

The key length.

Required	Default Value	Valid Values
Yes	N/A	Varies depending on key type. The supported DSA key lengths are 512 bits and 1024 bits. The supported ECDSA key lengths are 256 bits, 384 bits, and 521 bits. The supported RSA key lengths are 1024 bits, 2048 bits, and 4096 bits.

## addTargetAccount

Use the **addTargetAccount** command to add a target account for credential management. In addition to the parameters in this topic, other parameters might be required, based on the Application Type and Target Connector that you configure.

For a description of these additional parameters, see the appropriate target connector topic. For example, see [Windows Remote Target Connector CLI Configuration](#) for target account parameters unique to Windows Remote.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=addTargetAccount
  TargetServer.hostName=myhostname.mydomain.com

TargetApplication.name=myApplication TargetAccount.userName=sysop1
  TargetAccount.password=sys0p2 TargetAccount.cacheBehavior=useCacheFirst

TargetAccount.cacheDuration=17 Attribute.descriptor1="Lab"
  Attribute.descriptor2="Ottawa"
```

## Parameters

### TargetServer.hostName

The host name for the target server on which the target account resides.

Required	Default Value	Valid Values
Either <code>TargetServer.hostName</code> and <code>TargetApplication.name</code> ; or <code>TargetApplication.ID</code> is required.	N/A	This value must match a target server name that is registered in Credential Manager.

### TargetApplication.name

The target application name on which the target account is hosted.

Required	Default Value	Valid Values
One of <code>TargetApplication.name</code> or <code>TargetApplication.ID</code> is required.	N/A	This value must match a target application name that is registered in Credential Manager.

### TargetApplication.ID

The target application ID on which the target account is hosted.

Required	Default Value	Valid Values
One of <code>TargetApplication.name</code> or <code>TargetApplication.ID</code> is required.	N/A	Use <code>searchTargetApplication</code> to retrieve the <code>TargetApplication.ID</code> .

### TargetAccount.userName

The user name for the target account.

Required	Default Value	Valid Values
yes	N/A	String. <code>TargetAccount.userName</code> must match exactly the user name in the target application.

**TargetAccount.password**

The password for the target account.

Required	Default Value	Valid Values
yes	N/A	The initial password must be the same as the password on the target account, unless a user with more privileges synchronizes this password. If a password policy is associated with the target application, the password value must adhere to the password policy. In addition to compliance with password policy constraints, a password must be a minimum of 1 character and a maximum of 255 characters.

**TargetAccount.cacheAllow**

This parameter is deprecated. Use `TargetAccount.cacheBehavior`. Set `TargetAccount.cacheAllow=true` to have credentials for this account that is cached in the Credential Manager client.

Required	Default Value	Valid Values
no	true	true, false

**TargetAccount.cacheBehavior**

To cache the credentials for this account in the Credential Manager client and used first, set this parameter to `useCacheFirst`. If the command is set to `useServerFirst`, the credentials for this account are cached in the Credential Manager client but the server is contacted first. To ensure that the credentials for this account are not cached in the Credential Manager client, set this parameter to `noCache`.

Required	Default Value	Valid Values
no	<code>useCacheFirst</code>	<code>useCacheFirst</code> , <code>useServerFirst</code> , <code>noCache</code>

**TargetAccount.cacheDuration**

Use `TargetAccount.cacheDuration` to specify the number of days the account credentials are permitted to reside in a Credential Manager client cache.

Required	Default Value	Valid Values
no	30	1 - 356

**TargetAccount.privileged**

Set `TargetAccount.privileged=true` to indicate that this account is a privileged account. Set `TargetAccount.privileged=false` to indicate that this account is an application-to-application account.

Required	Default Value	Valid Values
no	false	true, false

**TargetAccount.accessType**

Use this text field for reference purposes.

Required	Default Value	Valid Values
no	N/A	String.

**TargetAccount.synchronize**

Set `TargetAccount.synchronize=true` to indicate that the password that is stored in Credential Manager should be synchronized with the password on the target system. This functionality is not supported with Target Application Type Generic. This functionality is not supported when `TargetAccount.compoundAccount=true`.

Required	Default Value	Valid Values
no	false	true, false

**Attribute.descriptor1**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

**Attribute.descriptor2**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

**PasswordViewPolicy.name**

The name of a Password View Policy that is attached to this account.

Required	Default Value	Valid Values
no	The system default Password View Policy	String

**TargetAlias.name**

A comma separated list of `TargetAlias.name` values. This parameter depends on the value of `useTargetAliasNameParameter` being true.

Required	Default Value	Valid Values
no	N/A	comma-separated String values

**useTargetAliasNameParameter**

A flag of true adds or deletes Target Aliases for this account using the values that are specified in the `TargetAlias.name` parameter.

Required	Default Value	Valid Values
no.	false	true, false



**TargetAccount.compoundAccount**

A flag of true adds or deletes Compound Target Servers for this account using the values that are specified in the `TargetAccount.compoundServerIDs` parameter.

Required	Default Value	Valid Values
no.	false	true, false

**TargetAccount.compoundServerIDs**

List of target server IDs to use as compound servers.

Required	Default Value	Valid Values
no.	n/a	comma-separated target server ID values

**passwordIsBase64Encoded**

A flag of true indicates that the specified password has been Base 64-encoded and should be decoded before being stored.

Required	Default Value	Valid Values
no.	false	true, false

**addTargetAlias**

Use the `addTargetAlias` command to add a target alias to Privileged Access Manager Credential Manager.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addTargetAlias
  TargetServer.hostName=myhostname.mydomain.com

TargetApplication.name=myApplication TargetAccount.userName=sysop1
TargetAlias.name=myaliasname
```

**Parameters****TargetServer.hostName**

The host name for the target server on which the target account resides.

Required	Default Value	Valid Values
Either <code>TargetServer.hostName</code> , <code>TargetApplication.name</code> , and <code>TargetApplication.name</code> ; or <code>TargetApplication.ID</code> is required.	N/A	This value must match a target server name that is registered in Credential Manager.

**TargetApplication.name**

The target application name on which the target account is hosted.

Required	Default Value	Valid Values
Either TargetServer.hostName, TargetApplication.name, and TargetApplication.name; or TargetApplication.ID is required.	N/A	This value must match a target application name that is registered in Credential Manager.

### **TargetAccount.userName**

The account user name that is associated with the target alias.

Required	Default Value	Valid Values
Either TargetServer.hostName, TargetApplication.name, and TargetApplication.name; or TargetApplication.ID is required.	N/A	This value must match a target account name that is registered in Credential Manager.

### **TargetAccount.ID**

The account ID associated with the target alias.

Required	Default Value	Valid Values
Either TargetServer.hostName, TargetApplication.name, and TargetApplication.name; or TargetApplication.ID is required.	N/A	Use searchTargetAccount to retrieve the TargetAccount.ID.

### **TargetAlias.name**

The name of this target alias.

Required	Default Value	Valid Values
yes	N/A	String. The target alias name must be unique within the Credential Manager server.

## **addTargetApplication**

Use the `addTargetApplication` command to add a target application to Credential Manager. More parameters may be required, depending upon the Target Application Type.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addTargetApplication
```

```
TargetServer.hostName=myhostname.mydomain.com
```

```
TargetApplication.name=myApplication
```

```
TargetApplication.type=unixII Attribute.descriptor1="Vienna"
```

```
Attribute.descriptor2="Lab"
```

**Parameters****TargetServer.ID**

The ID of the target server on which the target application is hosted.

Required	Default Value	Valid Values
TargetServer.ID or TargetServer.hostName is required.	N/A	Use searchTargetServer to retrieve the TargetServer.ID.

**TargetServer.hostName**

The host name for the target server on which the target application resides.

Required	Default Value	Valid Values
TargetServer.ID or TargetServer.hostName is required.	N/A	This value must match a target server name that is registered in Credential Manager.

**TargetApplication.name**

The name of the target application.

Required	Default Value	Valid Values
yes	N/A	The target application name must be unique for a given target server.

**TargetApplication.type**

The target application connector name. Valid values depend upon which target connectors are installed on your system.

Required	Default Value	Valid Values
yes	N/A	Turnkey target connectors include: cisco, CiscoSSH, ldap, mssql, oracle, sybase, unixII (capitalize "i " twice after "unix "), unixAccountViaTelnet, windows, windowsDomainService . In addition, your system may contain custom target connectors.

**PasswordPolicy.name**

The name of the password policy that is associated with accounts belonging to this application.

Required	Default Value	Valid Values
no	null	If a password policy is not specified, manually entered passwords are not validated against a policy. In addition, Credential Manager generated passwords use the Credential Manager default password policy.

### **PasswordPolicy.ID**

The ID of the password policy that is associated with accounts belonging to this application.

Required	Default Value	Valid Values
no	null	Use <code>searchPasswordPolicy</code> to retrieve the <code>PasswordPolicy.ID</code> . If a password policy is not specified, manually entered passwords are not validated against a policy. In addition, Credential Manager generated passwords use the Credential Manager default password policy.

### **Attribute.descriptor1**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

### **Attribute.descriptor2**

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String.

### **Attribute.enableAutoConnectTargetAccount**

A Boolean value to enable / disable `autoConnectTargetAccount` for an application instance.

Required	Default Value	Valid Values
no	false	true or false

## **addTargetServer**

Use the `addTargetServer` command to add a target server to Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addTargetServer
TargetServer.hostName=myhostname.mydomain.com
```

```
Attribute.descriptor1="Lab" Attribute.descriptor2="Vienna"
```

## Parameters

### TargetServer.hostName

The host name for the target server.

Required	Default Value	Valid Values
yes	N/A	This must be the fully qualified host name as entered in the DNS server.

### TargetServer.deviceName

The device name for the target server.

Required	Default Value	Valid Values
no	Same as host name if not specified.	String

### Attribute.descriptor1

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String

### Attribute.descriptor2

A text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no	N/A	String

## addUser

Use the addUser command to add a Credential Manager user account. The Windows CLI allows up to nine parameters, including the mandatory adminUserID and cspmHostName. To enter the addUser command with more than nine parameters, use the batchSequence command with an XML formatted input file.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=addUser
User.userID=demo User.password="demo123$" User.authenticationType=CSPM

User.status=ACTIVE User.userGroupIDS=2 User.firstName=Demo User.lastName=User
User.email=jdoe@xceedium.com User.viewType=admin
```

**NOTE**

If you add a suspended user, then the user's deactivation reason is automatically set to **Other** in the UI.

**Parameters****User.userID**

The user name of the Credential Manager user.

Required	Default Value	Valid Values
yes	N/A	String.

**User.password**

The user's password.

Required	Default Value	Valid Values
This parameter is required if the authentication type is Privileged Access Manager Credential Manager.	N/A	String. Credential Manager passwords must contain 6-16 characters containing at least one alphabetic, one numeric, and one special character.

**User.authenticationType**

Authentication type of the user.

Required	Default Value	Valid Values
no	CSPM	CSPM, LDAP, SecurID, Kerberos, X509, or any installed authentication connector. See \$CSPM_SERVER_HOME/cspmserver/config/authentication.xml for a complete list of installed authentication connectors.

**User.status**

Set User.status=ACTIVE for active user accounts and User.Status=SUSPENDED to suspend a user account.

Required	Default Value	Valid Values
no	ACTIVE	ACTIVE or SUSPENDED

**User.userGroupIDS**

IDs of the User Groups to assign to this user.

Required	Default Value	Valid Values
no	null	Numeric IDs delimited by comma. Use searchUserGroups to retrieve user group IDs. Alternatively, you can specify the User.userGroupNames parameter. Values must match user groups that are registered in Credential Manager.

**User.userGroupNames**

Names of the User Groups to assign to this user.

Required	Default Value	Valid Values
no	null	String. A comma-delimited list of user group names.

**User.firstName**

First name of the user.

Required	Default Value	Valid Values
no	N/A	String.

**User.lastName**

Last name of the user.

Required	Default Value	Valid Values
no	N/A	String.

**User.email**

Email address of the user.

Required	Default Value	Valid Values
mandatory no	N/A	String.

**User.viewType**

Determines what GUI view this user has access to - administrative or general.

Required	Default Value	Valid Values
no	N/A	admin, general

**addUserGroup**

Use the addUserGroup command to add a credential group to Credential Manager.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=addUserGroup
  UserGroup.name=OttUserGroup UserGroup.description="Ottawa user group"
  UserGroup.roleID=11 UserGroup.groups=3,4
```

**Parameters****UserGroup.name**

The user group name.

Required	Default Value	Valid Values
yes	N/A	String. A unique Name in Credential Manager

### **UserGroup.description**

Description of the group.

Required	Default Value	Valid Values
no	N/A	String.

### **UserGroup.roleID**

The role identifier of this group.

Required	Default Value	Valid Values
yes	N/A	This value must match a role ID registered in Credential Manager.

### **UserGroup.groups**

An ArrayList of String values or a string ArrayList, each element containing a string value of a group ID.

Required	Default Value	Valid Values
no	true	N/A

#### **NOTE**

Each dynamic target group referenced in the listed group IDs *must have at least one* filter defined. If not, the group is not created.

### **UserGroup.readOnly**

The read-only flag for this user group. Warning, read-only cannot be deleted if you make a mistake.

Required	Default Value	Valid Values
no	false	true or false

## **archiveAuditData**

Use the `archiveAuditData` command to remove audit data up to the specified end date from the Credential Manager database and write it to a file.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=archiveAuditData
endDate=2018-11-01 storage=failover
```



**Parameters*****endDate***

All metric data up to and including the end date is removed from the Credential Manager database and stored in the archive file.

Required	Default Value	Valid Values
yes	N/A	YYYY-MM-DD

***storage***

Designate the mounted external storage for the archived data. This storage is either a primary or the failover storage that is established with the supported mount types. The external storage must be mounted and available for this command to succeed.

Required	Default Value	Valid Values
yes	N/A	Primary, Failover

***folder***

The name of the additional folder, or folders created at the root of the mounted external storage for the archived data.

Required	Default Value	Valid Values
no	blank	directory path

***fileName***

The file name (including the path) where the archive data is stored. If the file does not exist, it is created. Otherwise, data is appended. If not specified, this command creates a file in the external space that is indicated by the storage/folder parameters. The date stamp on the default file indicates the date/time when the archive command was issued, not the end archive date. `Hardware-id` is the Hardware ID found on the **Configuration, Licensing** page and the **System Info, Hardware Identifiers** page.

Required	Default Value	Valid Values
no	cspmserver_ <i>hardware-id</i> _auditlog_YYYY-MM-DD-HHMMSS	File path

***resultLimit***

The limit for the number of database records to be processed at a time. Set to -1 to specify no limit. **Caution:** A large value results in a larger rollback segment being allocated for each database transaction.

Required	Default Value	Valid Values
no	100	Integer

***compress***

Determine whether the archive results file should be compressed (gz file).

Required	Default Value	Valid Values
no	true	true, false

## archiveMetricData

Use the `archiveMetricData` command to remove metric data up to the specified end date from the Credential Manager database and write it to a file.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=archiveMetricData
  endDate=2018-01-01 storage=primary compress=false
```

### Parameters

#### *endDate*

All metric data up to and including the end date is removed from the Credential Manager database and stored in the archive file.

Required	Default Value	Valid Values
yes	N/A	YYYY-MM-DD

#### *storage*

Designate the mounted external storage for the archived data. This storage is either a primary or the failover storage that is established with the supported mount types. The external storage must be mounted and available for this command to succeed.

Required	Default Value	Valid Values
yes	N/A	Primary, Failover

#### *folder*

The name of the additional folder, or folders created at the root of the mounted external storage for the archived data.

Required	Default Value	Valid Values
no	blank	directory path

#### *fileName*

The file name (including the path) where the archive data is stored. If the file does not exist, it is created. Otherwise, data is appended. If not specified, this command creates a file in the external space that is indicated by the storage/folder parameters. The date stamp on the default file indicates the date/time when the archive command was issued, not the end archive date. `Hardware-id` is the Hardware ID found on the **Configuration, Licensing** page and the **System Info, Hardware Identifiers** page.

Required	Default Value	Valid Values
no	cspmserver_ <i>hardware-id</i> _metric_YYYY-M M-DD-HHMMSS	File path

#### *resultLimit*

The limit for the number of database records to be processed at a time. Set to -1 to specify no limit. **Caution:** A large value results in a larger rollback segment being allocated for each database transaction.

Required	Default Value	Valid Values
no	100	Integer

### ***compress***

Determine whether the archive results file should be compressed (gz file).

Required	Default Value	Valid Values
no	true	true, false

## **batchSequence**

Use the batchSequence command for bulk registration. The input to the batchSequence command is an XML formatted file.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=batchSequence
inputfile=myinput.xml outputfile=results.xml
```

## **Parameters**

### **inputfile**

The file containing the bulk registration input. The XML format for the input file is documented in [Credential Manager XML Schema for Batch Processing](#).

Required	Default Value	Valid Values
yes	N/A	String.

### **outputfile**

The file containing the XML formatted output result. If this parameter is not included, the output is sent to standard out.

Required	Default Value	Valid Values
no	standard output	String.

### **stopOnError**

Set stopOnError=true to indicate that the batch sequence is stopped when an error is encountered. Set stopOnError=false to indicate that the batch sequence continues with the next command when an error is encountered. If the data in the input file has dependencies, set stopOnError=true.

Required	Default Value	Valid Values
no	false	true, false

**multipleTransactions**

Set multipleTransactions=true to indicate that the batch sequence is treated as its own transaction. Set multipleTransactions=false to indicate that the batch sequence is treated as a single transaction. When the batch sequence is treated as a single transaction (multipleTransactions=false) the stopOnError is overridden to be true.

Required	Default Value	Valid Values
no	true	true, false

**canGetCredentials**

Use the canGetCredentials command to validate the ability of a specific script to retrieve credentials without making a credential request. This command does not verify the fingerprint of the request server or the requesting script hash. This command returns "Success 1" when the query result is true and "Success 0" when the query result is false.

Authorization mappings settings determine which values are validated. For example, if check execution ID is not set, then the execution ID parameter value does not affect the output result. The Windows CLI allows up to nine parameters, including mandatory adminUserID and cspmHostName. To invoke this command with more than nine parameters, use the batchSequence command with an XML formatted input file.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=canGetCredentials
  TargetAlias.name=myalias1 RequestScript.name=example.pl
```

```
RequestScript.filePath=/usr/tmp/examples RequestScript.executionPath=/usr/tmp/
examples Authorization.executionUser=admin
```

```
RequestServer.hostName=myhostname.mydomain.com RequestServer.osName=win
```

**Parameters****TargetAlias.name**

Alias name for which you want to validate the ability to get credentials.

Required	Default Value	Valid Values
yes	N/A	String

**RequestScript.name**

Name of the requesting script.

Required	Default Value	Valid Values
yes	N/A	String

**RequestScript.filePath**

File path where the requesting script resides.

Required	Default Value	Valid Values
no	N/A	String

### **RequestScript.executionPath**

Path from which the requesting script is run.

Required	Default Value	Valid Values
yes	N/A	String

### **Authorization.executionUser**

Username with which the requesting script will be run.

Required	Default Value	Valid Values
yes	N/A	String

### **RequestServer.hostName**

Request server hostname on which the requesting script is located.

Required	Default Value	Valid Values
yes	N/A	String

### **RequestServer.osName**

Operating System name for the request server host. Set this value if the Operating System is Windows. Any other value sets the Operating System as UNIX-based.

Required	Default Value	Valid Values
no	unix	win, unix

## **checkConnectionStatus**

Use the checkConnectionStatus command to check the status of a client.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=checkConnectionStatus
RequestServer.ID=1000
```

### **Parameter**

#### ***RequestServer.ID***

The ID of the target server being checked

Required	Default Value	Valid Values
Yes	N/A	integer

## checkDelete

Use the checkDelete command to determine if a target server or request server can be deleted or was previously deleted.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=checkDelete TargetServer.ID=1002
RequestServer.ID=1001
```

### Parameters

#### TargetServer.ID

The ID of the target server being checked

Required	Default Value	Valid Values
One or both of TargetServer.ID or RequestServer.ID is required	N/A	int.

#### RequestServer.ID

The ID of the request server being checked

Required	Default Value	Valid Values
One or both of TargetServer.ID or RequestServer.ID is required	N/A	int.

## checkInAccountPassword

Use the checkInAccountPassword command to check in a target account. This command can be run on a secondary site.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=checkInAccountPassword TargetAccount.ID=1
```

### Parameter

#### TargetAccount.ID

The user name for the target account.

Required	Default Value	Valid Values
yes	N/A	Integer. Identity of the target account.

## deleteAuthorization

Use the deleteAuthorization command to delete an existing authorization mapping.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteAuthorization
RequestServer.hostName=myhostname.mydomain.com RequestScript.name=example.pl
RequestScript.executionPath=/usr/tmp/examples TargetAlias.name=mytargetalias
```

**Parameters****Authorization.ID**

The unique identifier of the Authorization mapping.

Required	Default Value	Valid Values
TargetAlias.name, RequestServer.hostName, RequestScript.name, and RequestScript.executionPath or Authorization.ID is required.	N/A	Use searchAuthorization to retrieve the Authorization.ID.

**TargetAlias.name**

The target alias name.

Required	Default Value	Valid Values
Either TargetAlias.name or Authorization.targetGroupName is required	N/A	This value must match the target alias name that is registered in Credential Manager.

**RequestServer.hostName**

The request server host name on which the requesting application resides.

Required	Default Value	Valid Values
One of Authorization.requestGroupName, RequestServer.hostName, or RequestServer.hostName/ RequestScript.name/ RequestScript.executionPath	N/A	This value must match the request server name that is registered in Credential Manager.

**RequestScript.name**

The requesting application name.

Required	Default Value	Valid Values
One of Authorization.requestGroupName, RequestServer.hostName, or RequestServer.hostName/ RequestScript.name/ RequestScript.executionPath	N/A	This value must match the script name that is registered in Credential Manager.

**RequestScript.executionPath**

The requesting application execution path, as registered in Credential Manager.

Required	Default Value	Valid Values
One of Authorization.requestGroupName, RequestServer.hostName, or RequestServer.hostName/RequestScript.name/RequestScript.executionPath	N/A	This value must match the script execution path registered in Credential Manager.

### **Authorization.targetGroupName**

The target group name.

Required	Default Value	Valid Values
TargetAlias.name or Authorization.targetGroupName is required	N/A	This value must match the target group name that is registered in Credential Manager.

### **Authorization.requestGroupName**

The request group name.

Required	Default Value	Valid Values
One of Authorization.requestGroupName, RequestServer.hostName, or RequestServer.hostName/RequestScript.name/RequestScript.executionPath	N/A	This value must match the request group name that is registered in Credential Manager.

## **deleteFilter**

Use the deleteFilter command to delete a filter from a target group or request group. The group must first be added using the addGroup command.

### **Example**

```
capapm_command capam=capamServer adminUserID=admin cmdName=deleteFilter
Filter.ID=6
```

## **Parameters**

### **Filter.ID**

The Id of the request or target group

Required	Default Value	Valid Values
yes	N/A	N/A



## deleteGroup

Use the deleteGroup command to delete a target or request group. This command automatically deletes filters associated with this group.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteGroup Group.ID=3
```

### Parameters

#### Group.ID

ID of the group you wish to delete.

Required	Default Value	Valid Values
One of Group.name or Group.ID is required.	N/A	Numeric. This value must match the group ID registered in Credential Manager.

#### Group.name

The group name.

Required	Default Value	Valid Values
One of Group.name or Group.ID is required.	N/A	String. This value must match the group name registered in Credential Manager.

#### Group.type

The group type.

Required	Default Value	Valid Values
Optional unless Group.name is specified, and that value is not unique.	N/A	String. This value must match the group type registered in Credential Manager.

## deletePasswordPolicy

Use the deletePasswordPolicy command to delete a password policy.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deletePasswordPolicy
PasswordPolicy.name=passwordPolicyName
```

### Parameters

#### PasswordPolicy.ID

The ID of the password policy.

Required	Default Value	Valid Values
yes or PasswordPolicy.name	null	Numeric

#### PasswordPolicy.name

The name of the password policy.

Required	Default Value	Valid Values
yes or PasswordPolicy.ID	null	String

## deletePasswordViewPolicy

Use the deletePasswordViewPolicy command to delete a password view policy from Privileged Access Manager Credential Manager.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deletePasswordViewPolicy
PasswordViewPolicy.name=restrictedAccounts
```

### Parameters

#### PasswordViewPolicy.ID

The ID of the password view policy.

Required	Default Value	Valid Values
One of PasswordViewPolicy.ID or PasswordViewPolicy.name is required	N/A	The ID of a password view policy in Credential Manager. Use searchPasswordViewPolicy to retrieve the PasswordViewPolicy.ID.

#### PasswordViewPolicy.name

The name of the password view policy.

Required	Default Value	Valid Values
One of PasswordViewPolicy.ID or PasswordViewPolicy.name is required	N/A	A text string matching the name of a password view policy in Credential Manager.

## deletePasswordViewRequest

Use the deletePasswordViewRequest command to delete either a specific password view request or all expired password view requests

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deletePasswordViewRequest
PasswordViewRequest.ID=1,2,3
```

### Parameters

#### PasswordViewRequest.ID

The ID of a password view request. Allow to input in comma separated format, such as, id2,id3,id5 etc

Required	Default Value	Valid Values
no	N/A	passwordviewrequestid from PasswordViewRequest table

## **deleteRequestScript**

Use the deleteRequestScript command to delete an existing requesting application. Requesting applications cannot be deleted if there is an authorization mappings associated with the application.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteRequestScript RequestScript.ID=7,8
```

## **Parameters**

### **RequestScript.ID**

The requesting application ID you wish to delete. This parameter may contain a comma separate list.

Required	Default Value	Valid Values
Either RequestScript.ID; or RequestServer.hostName, RequestScript.name, and RequestScript.executionPath is required.	N/A	Use searchRequestScript to retrieve the RequestScript.ID.

### **RequestServer.hostName**

The request server host name on which the requesting application resides.

Required	Default Value	Valid Values
Either RequestScript.ID; or RequestServer.hostName, RequestScript.name, and RequestScript.executionPath is required.	N/A	This value must match the request server name registered in Credential Manager.

### **RequestScript.name**

The requesting application name.

Required	Default Value	Valid Values
Either RequestScript.ID; or RequestServer.hostName, RequestScript.name, and RequestScript.executionPath is required.	N/A	String.

### **RequestScript.executionPath**

The location from which the requesting application will be executed.

Required	Default Value	Valid Values
Either RequestScript.ID; or RequestServer.hostName, RequestScript.name, and RequestScript.executionPath is required.	N/A	String.

## deleteRequestServer

Use the deleteRequestServer command to delete an existing request server from Credential Manager. You cannot delete a request server if there are any authorization mappings or request scripts associated with the request server.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteRequestServer
RequestServer.hostName=myhostname.mydomain.com
```

### Parameters

#### RequestServer.hostName

The host name of the request server.

Required	Default Value	Valid Values
RequestServer.hostName, RequestServer.hostName, or RequestServer.ID is required.	N/A	This value must match a request server name registered in Credential Manager.

#### RequestServer.deviceName

The device name of the request server.

Required	Default Value	Valid Values
RequestServer.hostName, RequestServer.hostName, or RequestServer.ID is required.	N/A	This value must match a request server name registered in Credential Manager.

#### RequestServer.ID: The unique ID for the request server.

Required	Default Value	Valid Values
RequestServer.hostName, RequestServer.hostName, or RequestServer.ID is required.	N/A	Use searchRequestServer to retrieve the RequestServer.ID.

## deleteRequestServerDefaults

Use the deleteRequestServerDefaults command to delete a request server defaults in Credential Manager.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteRequestServerDefaults
RequestServerDefaults.ID=1001
```

**Parameters****RequestServerDefaults.ID**

The id of the record to delete.

Required	Default Value	Valid Values
yes	N/A	Integer

**deleteRole**

Use the deleteRole command to delete roles from Credential Manager.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteRole Role.ID=11
```

**Parameters****Role.ID**

The unique ID of the role or a comma delimited list of roles you wish to delete.

Required	Default Value	Valid Values
yes	N/A	Numeric.

**deleteSSHKeyPairPolicy**

Use the deleteSSHKeyPairPolicy command to delete an SSH Key Pair policy.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteSSHKeyPairPolicy
SSHKeyPairPolicy.name=MySSHKeyPairPolicy
```

**Parameters****SSHKeyPairPolicy.ID**

The ID of the SSH Key Pair policy.

Required	Default Value	Valid Values
Yes if SSHKeyPairPolicy.name is not specified	N/A	Numeric or a String of comma-separated numeric values

**SSHKeyPairPolicy.name**

The name of the SSH Key Pair policy.

Required	Default Value	Valid Values
Yes if SSHKeyPairPolicy.ID is not specified	N/A	String

## deleteSystemProperty

Use the deleteSystemProperty command to delete a system property (that is, set isDeleted = 1).

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteSystemProperty propertyName=test
```

### Parameters

#### propertyName

The property key name.

Required	Default Value	Valid Values
yes	N/A	A valid value is one that exists in the system properties table.

## deleteTargetAccount

Use the deleteTargetAccount command to delete an existing target account from Credential Manager. Target accounts cannot be deleted if there is an authorization mapping associated with the account. Deleting a target account automatically deletes any target aliases associated with the account.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteTargetAccount
  TargetServer.hostName=myhostname.mydomain.com

  TargetApplication.name=myApplication TargetAccount.userName=sysopl
```

### Parameters

#### TargetServer.hostName

The host name of the target server on which the target application is hosted.

Required	Default Value	Valid Values
Either TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID is required.	N/A	This value must match a target server name registered in Credential Manager.

#### TargetApplication.name

The target application name on which the target account is hosted.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID is required.	N/A	This value must match a target application name registered in Credential Manager.

**TargetAccount.userName**

The user name for the target account.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID is required.	N/A	This value must match a target account name registered in Credential Manager.

**TargetAccount.ID**

The ID for the target account.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID is required.	N/A	Use searchTargetAccount to retrieve the TargetAccount.ID.

**deleteTargetAlias**

Use the deleteTargetAlias command to delete an existing target alias from the Credential Manager server. Target aliases cannot be deleted if there is an authorization mapping associated with the alias.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteTargetAlias TargetAlias.ID=12
```

**Parameters****TargetAlias.name**

The target alias name. This parameter is required if TargetAlias.ID is not specified.

Required	Default Value	Valid Values
TargetAlias.name or TargetAlias.ID is required.	N/A	The target alias name must match a target alias registered in Credential Manager.

**TargetAlias.ID**

The target alias unique identifier.

Required	Default Value	Valid Values
TargetAlias.name or TargetAlias.ID is required.	N/A	Use searchTargetAlias to retrieve the TargetAlias.ID.

**deleteTargetApplication**

Use the deleteTargetApplication command to delete an existing target application from Credential Manager. Target applications cannot be deleted if there is an authorization mapping associated with the application. Deleting a target application automatically deletes any target accounts and target aliases associated with the application.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteTargetApplication
TargetServer.hostName=myhostname.mydomain.com TargetApplication.name=myApplication
```

**Parameters****TargetServer.hostName**

The host name of the target server on which the target application is hosted.

Required	Default Value	Valid Values
TargetServer.hostName and TargetApplication.name; or TargetApplication.ID is required.	N/A	This value must match a target server name registered in Credential Manager.

**TargetApplication.name**

The target application name.

Required	Default Value	Valid Values
TargetServer.hostName and TargetApplication.name; or TargetApplication.ID is required.	N/A	This value must match a target application name registered in Credential Manager.

**TargetApplication.ID**

The target application ID.

Required	Default Value	Valid Values
TargetServer.hostName and TargetApplication.name; or TargetApplication.ID is required.	N/A	Use searchTargetApplication to retrieve the TargetApplication.ID.

**deleteTargetServer**

Use the deleteTargetServer command to delete an existing target server from Credential Manager. A target server cannot be deleted if there is a target alias associated with the server. Deleting a target server automatically deletes any target applications and target accounts associated with the server, never any aliases.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteTargetServer
TargetServer.hostName=myhostname.mydomain.com
```

**Parameters****TargetServer.ID**

The ID for the target server, or a comma-separated list of IDs.

Required	Default Value	Valid Values
TargetServer.ID, TargetServer.hostName, or TargetServer.deviceName is required.	N/A	Use searchTargetServer to retrieve the TargetServer.ID.



**TargetServer.hostName**

The host name of the target server.

Required	Default Value	Valid Values
TargetServer.ID, TargetServer.hostName, or TargetServer.deviceName is required.	N/A	String. This value must match a target server name registered in Credential Manager.

**TargetServer.deviceName**

The device name of the target server.

Required	Default Value	Valid Values
TargetServer.ID, TargetServer.hostName, or TargetServer.deviceName is required.	N/A	String. This value must match a target server name registered in Credential Manager.

**deleteUser**

Use the deleteUser command to delete a user account or list of user accounts.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteUser User.userID=demo
```

**Parameters****User.userID**

The user name of the Credential Manager user to be deleted or a comma delimited list of user names to be deleted.

Required	Default Value	Valid Values
yes	N/A	String

**deleteUserGroup**

Use the deleteUserGroup command to delete a user group.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=deleteUserGroup UserGroup.ID=18
```

**Parameters****UserGroup.ID**

The user group ID or a comma delimited list of user group IDs you wish to delete.

Required	Default Value	Valid Values
UserGroup.ID or UserGroup.name is required.	N/A	Numeric. A unique user group ID in Credential Manager.

**UserGroup.name**

The name of the user group.

Required	Default Value	Valid Values
UserGroup.ID or UserGroup.name is required.	N/A	String. A unique user group name in Credential Manager.

## disableCLIHostNameCheck

Use the disableCLIHostNameCheck command to disable host name checking when connecting via the CLI.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=disableCLIHostNameCheck
```

## disableFingerprinting

Use the disableFingerprinting command to disable hardware fingerprinting for request servers (Credential Manager clients). This command has no parameters. By default, this feature is disabled.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=disableFingerprinting
```

## enableCLIHostNameCheck

Use the enableCLIHostNameCheck command to force host name checking when connecting via the CLI.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=enableCLIHostNameCheck
```

## enableFingerprinting

Use the enableFingerprinting command to enable hardware fingerprinting for request servers (Credential Manager clients). This command has no parameters. By default, this feature is disabled.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=enableFingerprinting
```

## enableLicense

Use the enableLicense command to activate your Credential Manager server license.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=enableLicense license=dae1993ace1473a...
```

## Parameter

### license

A Credential Manager server license string. See your CA Technologies sales representative.

Required	Default Value	Valid Values
yes	N/A	String

## expirePasswordViewRequest

Use the expirePasswordViewRequest command to expires a password view request.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=expirePasswordViewRequest
PasswordViewRequest.ID=1000
```

### Parameter

#### PasswordViewRequest.ID

The ID of the password view request.

Required	Default Value	Valid Values
yes	N/A	Numeric vaue

## forceCheckInAccountPassword

Use the forceCheckInAccountPassword command to check in a target account checked out by another user. This command can be run on a secondary site.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=forceCheckInAccountPassword
TargetAccount.ID=1
```

### Parameters

#### TargetAccount.ID

The ID of the target account you are checking in.

Required	Default Value	Valid Values
TargetAccount.ID or PasswordViewRequest.ID must be specified.	N/A	Use searchTargetAccount to retrieve the TargetAccount.ID.

#### PasswordViewRequest.ID

The ID of the target account you are checking in.

Required	Default Value	Valid Values
TargetAccount.ID or PasswordViewRequest.ID must be specified.	N/A	Use searchPasswordViewRequest or searchPasswordViewRequestByRequestor to retrieve the PasswordViewRequest.ID.

## generateEncryptedPassword

Use the `generateEncryptedPassword` command to encrypt the password found in Tomcat `server.xml`.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=generateEncryptedPassword
password=cspmpublic
```

### Parameters

#### password

The password that you want to encrypt.

Required	Default Value	Valid Values
yes	N/A	Any string

## getAllScriptHash

Use the `getAllScriptHash` command to refresh each of the script hashes for a given request server. A script hash value is a SHA-1 message digest value of the script (file).

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=getAllScriptHash
RequestServer.hostName=myhostname.mydomain.com
```

### Parameters

#### RequestServer.hostName

The host name of the request server.

Required	Default Value	Valid Values
RequestServer.hostName or RequestServer.ID is required.	N/A	String

#### RequestServer.ID

The ID of the request server.

Required	Default Value	Valid Values
RequestServer.hostName or RequestServer.ID is required.	N/A	Use <code>searchRequestServer</code> to retrieve the RequestServer.ID

## getAwsManagementConsoleSessionUrl

Use the `getAwsManagementConsoleSessionUrl` command to retrieve a URL to an authenticated Amazon Web Services Management Console federation session.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=getAwsManagementConsoleSessionUrl AWS.accessKeyID=AKIAIUHQMBKFCROZL5NQ
```

```
AWS.secretAccessKey=l2YaoK/or4Jffi+XTlCds0x5mLUdRoCTcvXb/e9y
AWS.consoleUrl=https://console.aws.amazon.com/sns
```

```
AWS.issuerUrl=https://www.xceedium.com/ AWS.signinUrl=https://
signin.aws.amazon.com/federation
```

```
AWS.sessionDuration=3600 AWS.policy={\"Statement\": [{\"Action\": \"sns:*\",
\\\"Effect\": \"Allow\", \"Resource\": \"*\"]}}
```

## Parameters

### **AWS.accessKeyID**

The AWS access key.

Required	Default Value	Valid Values
yes	N/A	^[A-Z0-9]{20}\$

### **AWS.secretAccessKey**

The AWS secret access key.

Required	Default Value	Valid Values
yes	N/A	^[a-zA-Z0-9]{40}\$

### **AWS.issuerUrl**

The URL to which the user should be redirected when their federation session expires.

Required	Default Value	Valid Values
yes	N/A	https://[a-zA-Z0-9]{1,256}([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?

### **AWS.consoleUrl**

The URL of the Management Console.

Required	Default Value	Valid Values
yes	N/A	https://[a-zA-Z0-9]{1,256}([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?([a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256} \.[a-zA-Z0-9]{1,256})?

### **AWS.signinUrl**

The URL of the AWS federated signin service.

Required	Default Value	Valid Values
yes	N/A	https:\V[0-9a-zA-Z]([-\.\w]*[0-9a-zA-Z])*(:(0-9)*)*(V?)([a-zA-Z0-9\-\.\?\\'\ /]+\&#38;\\$#\_)*?

### **AWS.policy**

A policy that applies to the federated user.

Required	Default Value	Valid Values
no	N/A	String

### **AWS.stsEndpoint**

The STS endpoint to use if specified; otherwise, use the default endpoint.

Required	Default Value	Valid Values
no	N/A	String

### **AWS.sessionDuration**

The duration, in seconds, that the federation session should last. Acceptable durations are in the interval [3600 .. 129600].

Required	Default Value	Valid Values
yes	N/A	Integer

### **AWS.urlEncodeOption**

Optionally encode the session URL.

Required	Default Value	Valid Values
no	false	Boolean

### **AWS.federatedUserName**

The name of the federated user to display in the AWS Management Console.

Required	Default Value	Valid Values
yes	N/A	String

## **getErrorCodes**

Use the getErrorCodes command to retrieve an XML list of Credential Manager error codes. This command takes no parameters.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=getErrorCodes
```

## getEventProcessingMetrics

Use the getEventProcessingMetrics command to get metrics for processing of notification events (events sent to clients or proxies). This information can determine the throughput of the overall Credential Manager system in processing events sent to clients and proxies. If you determine that the throughput is not high enough, you can deploy additional Credential Manager servers.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=getEventProcessingMetrics
samplePeriodMinutes=720
```

### Parameters

#### samplePeriodMinutes

Sample period in minutes.

Required	Default Value	Valid Values
no	1440	1 through 1440

## getLocalProperty

Use the getLocalProperty command to retrieve the property value which matches the property name.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=getLocalProperty propertyName=sitename
```

### Parameters

#### propertyName

The property key name.

Required	Default Value	Valid Values
yes	N/A	A valid value is one that exist in the local properties table.

## getMostRecentPasswordHistory

Use the getMostRecentPasswordHistory command to retrieve the most recent password history for a target account.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=getMostRecentPasswordHistory TargetAccount.ID=100
```

### Parameter

#### TargetAccount.ID

The ID of the Target Account.

Required	Default Value	Valid Values
yes	N/A	Use searchTargetAccount to retrieve the TargetAccount.ID

## getMSOLFederatedSessionCmd

Use the getMSOLFederatedSessionCmd command to retrieve a federated session request sent to the Microsoft Online (MSOL) portal. The request is returned as a web form that is automatically submitted by the browser. Submitting the form launches a federated session with MSOL.

### Example

```
capam_command capam=capamServer adminUserID=super adminPassword=<PASSWORD>
cmdName=getMsolFederatedSession
```

```
MSOL.portalUrl=https%3A//login.microsoftonline.com/login.srf
MSOL.stsEndpointUrl=https%3A//fs.xcdpoc.com/adfs/services/trust/2005/
usernamemixed
```

```
MSOL.stsEndpointReferenceUri=urn%3Afederation%3AMicrosoftOnline MSOL.wctx=MEST
%3D0%26LoginOptions%3D2%26wa%3Dwsignin1.0%26rpsnv%3D2%26ct%3D1361461138%26rver
%3D6.1.6206.0%26wp%3DMCMBI%26wreply
```

```
%3Dhttps:%252F%252Fportal.microsoftonline.com%252Flanding.aspx%253Ftarget%253D
%25252fdefault.aspx%26lc%3D1033%26id%3D271346%26
TargetAccount.ID=100
```

## Parameters

### MSOL.stsEndpointUrl

The URL of the Security Token Service (STS) endpoint from which the security token shall be requested. In general, specify the appropriate URL that is exposed by your Active Directory Federation Service (ADFS). The endpoint must support the WS-Trust 2005 (username mixed mode) protocol. For example, https://<ADFS-HOST>/adfs/services/trust/2005/usernamemixed.

Required	Default Value	Valid Values
yes	N/A	URL

### MSOL.stsEndpointReferenceUri

The reference URI to which the security token request applies. When ADFS is federated with MSOL, this value is typically "urn:federation:MicrosoftOnline" (without quotes).

Required	Default Value	Valid Values
yes	N/A	URI



**MSOL.portalUrl**

The URL of the MSOL portal. For example, <https://login.microsoftonline.com/login.srf>.

Required	Default Value	Valid Values
yes	N/A	URL

**MSOL.wctx**

This parameter contains context information that is relevant to MSOL. The value is derived by following the procedure for creating a smart link, which is described in Microsoft documentation. For additional instructions, please refer to <http://community.office365.com/en-us/wikis/sso/using-smart-links-or-idp-initiated-authentication-with-office-365.aspx>.

Required	Default Value	Valid Values
yes	N/A	String

**TargetAccount.ID**

The ID of the Target Account that represents the federated user's credentials. The username and password will be retrieved and sent to ADFS in a security token request. If ADFS successfully authenticates the credentials then it will issue a security token response that contains SAML assertions that are good for authenticating the federated user to MSOL.

Required	Default Value	Valid Values
yes	N/A	Use searchTargetAccount to retrieve the TargetAccount.ID

**reason**

The reason you are requesting a password view.

Required	Default Value	Valid Values
yes	N/A	String.

**reasonDetails**

Detailed description of why you wish to view the password.

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.requestPeriodStart**

If the account password view policy has dual authorization enabled, this parameter specifies the start time of the password view request.

Required	Default Value	Valid Values
no	N/A	Date string, of the format yyyy-MM-dd HH:mm

**PasswordViewRequest.requestPeriodEnd**

If the account password view policy has dual authorization enabled, this parameter specifies the end time of the password view request.

Required	Default Value	Valid Values
no	N/A	Date string, of the format yyyy-MM-dd HH:mm

### **referenceCode**

Displays the reference code.

Required	Default Value	Valid Values
no	N/A	String

## **getNumberOfAccounts**

Use the getNumberOfAccounts command to retrieve the number of target accounts registered in Credential Manager. This command takes no parameters.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=getNumberOfAccounts
```

## **getRequestServerDefaults**

Use the getRequestServerDefaults command to add a request server defaults to Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin  
cmdName=getRequestServerDefaults RequestServerDefaults.ID=1001
```

### **Parameters**

#### **RequestServerDefaults.ID**

The id of the record to get.

Required	Default Value	Valid Values
yes	N/A	Integer

## **getScriptHashAsynchronous**

Use the getScriptHashAsynchronous command to refresh a script hash for a specified request script on a request server (Credential Manager client). A script hash value is a SHA-1 message digest value of the script.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=getScriptHashAsynchronous RequestScript.ID=2
```

### **Parameters**

#### **RequestScript.ID**

The unique ID for the request script.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchRequestScript to retrieve the RequestScript.ID

### **getServiceStatus**

Use the getServiceStatus command to inquire the state of services associated with a Windows domain target account. This command assumes the service information is stored in an extend attribute named 'serviceInfo'.

#### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=getServiceStatus
TargetAccount.ID=24
```

### **Parameters**

#### **TargetAccount.ID**

The ID of the TargetAccount

Required	Default Value	Valid Values
Either TargetAccount.ID or TargetServer.hostName, TargetApplication.name and TargetAccount.userName is required.	N/A	integer

#### **TargetServer.hostName**

The host name of the TargetServer

Required	Default Value	Valid Values
Either TargetAccount.ID or TargetServer.hostName, TargetApplication.name and TargetAccount.userName is required.	N/A	String

#### **TargetApplication.name**

The name of the TargetApplication

Required	Default Value	Valid Values
Either TargetAccount.ID or TargetServer.hostName, TargetApplication.name and TargetAccount.userName is required.	N/A	String

### **TargetAccount.userName**

The user name of the TargetAccount

Required	Default Value	Valid Values
Either TargetAccount.ID or TargetServer.hostName, TargetApplication.name, TargetAccount.userName is required.	N/A	String

## **getSystemProperty**

Use the getSystemProperty to retrieve the property value which matches the property name.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=getSystemProperty
propertyName=DBVersion
```

### **Parameters**

#### **propertyName**

The property key name.

Required	Default Value	Valid Values
yes	N/A	A valid value is one that exists in the system properties table.

## **listCurrentPasswordViewRequestSummary**

Use the listCurrentPasswordViewRequestSummary command to list password view requests that are presently in force for the user executing the command.

Use the listCurrentPasswordViewRequestSummary command to list password view requests that are presently in force for the user executing the command (as an approver or a requester).

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=listCurrentPasswordViewRequestSummary
PasswordViewRequest.status="approved"
```

**Parameters**

You can use the following parameters with the `listCurrentPasswordViewRequestSummary` command.

**TIP**

Any parameter that contains a space must be enclosed between quotation marks.

***PasswordViewRequest.targetAccountID***

Filter results for the specified `targetAccountID`.

Required	Default Value	Valid Values
no	N/A	Integer

***PasswordViewRequest.targetAccountUserName***

Filter results for the specified `targetAccountUserName`.

Required	Default Value	Valid Values
no	N/A	String

***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checkin/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

***PasswordViewRequest.ssoType***

If specified with the value "Any", list only current password view requests made to use the password for access. Otherwise, list all current password view requests.

Required	Default Value	Valid Values
no	Null (no value specified)	"Any"

***Page.Number***

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

***Page.Size***

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.requestorID, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### ***Sort.Direction***

Sort.Direction specifies the order of the results. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## **listDBClusterMembers**

Use the listDBClusterMembers command to retrieve a list of all database cluster members in the system.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=listDBClusterMembers
```

## **listPasswordViewRequestByAccount**

Use the listPasswordViewRequestByAccount command to return a list of password view requests for a particular account.

### **Examples**

```
capam_command capam=capamServer adminUserID=admin
adminPassword=Myp@ss cmdName=listPasswordViewRequestByAccount
PasswordViewRequest.targetAccountID=1005
```

### **Parameters**

You can use the following parameters with the searchPasswordViewRequest command.

#### **TIP**

Any parameter that contains a space must be enclosed between quotation marks.

### ***PasswordViewRequest.ID***

Filter results for specified ID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestorID***

Filter results for specified requestorID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestorNameID***

Filter results for specified requestorNameID

Required	Default Value	Valid Values
no	N/A	String

### ***PasswordViewRequest.approverID***

Filter results for specified approverID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checked in or checked out:</b> "checkout" (or 4), "checkedin" (or 5)

### ***PasswordViewRequest.targetAccountID***

Filter results for specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.isCheckedOut***

Filter results for accounts that are checked out.

Required	Default Value	Valid Values
no	N/A	"true" or "false"

### ***PasswordViewRequest.ssoType***

Filter results by the specified SSO type.

Required	Default Value	Valid Values
no	N/A	"Browser", "RDP", "SSH", "VNC", "AWSAPI", "Telnet", "Other"

### ***Page.Number***

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

### ***Page.Size***

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.requestorID, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### ***Sort.Direction***

Sort.Direction specifies the order of the results. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## **listPasswordViewRequestByApproverSummary**

Use the listPasswordViewRequestByApproverSummary command to return a list of password view requests for which you are an approver.



## Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=listPasswordViewRequestByApproverSummary
```

## Parameters

You can use the following parameters with the searchPasswordViewRequest command.

### TIP

Any parameter that contains a space must be enclosed between quotation marks.

### ***PasswordViewRequest.ID***

Filter results for specified ID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestorID***

Filter results for specified requestorID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestorNameID***

Filter results for specified requestorNameID

Required	Default Value	Valid Values
no	N/A	String

### ***PasswordViewRequest.approverID***

Filter results for specified approverID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checked in/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

#### ***PasswordViewRequest.targetAccountID***

Filter results for specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

#### ***PasswordViewRequest.targetAccountUserName***

Filter results for specified target account user name.

Required	Default Value	Valid Values
no	N/A	String

#### ***PasswordViewRequest.ssoType***

Filter results the specified SSO type.

Required	Default Value	Valid Values
no	N/A	"Browser", "RDP", "SSH", "VNC", "AWSAPI", "Telnet", "Other"

#### ***Page.Number***

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

#### ***Page.Size***

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

#### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.requestorID, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### **Sort.Direction**

Sort.Direction specifies the order of the results. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## **listPasswordViewRequestByRequestorSummary**

Use the listPasswordViewRequestByRequestorSummary command to return a list of password view requests for which you are an approver.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=listPasswordViewRequestByRequestorSummary
```

### **Parameters**

You can use the following parameters with the searchPasswordViewRequest command.

#### **TIP**

Any parameter that contains a space must be enclosed between quotation marks.

### **PasswordViewRequest.ID**

Filter results for specified ID.

Required	Default Value	Valid Values
no	N/A	Integer

### **PasswordViewRequest.approverID**

Filter results for specified approverID.

Required	Default Value	Valid Values
no	N/A	Integer

### **PasswordViewRequest.approverNameID**

Filter results for specified approverNameID (for approved password view requests).

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.status**

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checked in or checked out:</b> "checkout" (or 4), "checkedin" (or 5)

**PasswordViewRequest.targetAccountID**

Filter results for specified target account ID (for approved password view requests).

Required	Default Value	Valid Values
no	N/A	Integer

**PasswordViewRequest.targetAccountUserName**

Filter results for the specified target account user name.

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.policyApproverID**

Filter results for the specified policy approver ID (for unapproved password view requests).

Required	Default Value	Valid Values
no	N/A	Integer

**PasswordViewRequest.ssoType**

Filter results for specified SSO type.

Required	Default Value	Valid Values
no	N/A	"Browser", "RDP", "SSH", "VNC", "AWSAPI", "Telnet", "Other"

**Page.Number**

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

**Page.Size**

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.requestorID, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### ***Sort.Direction***

Sort.Direction specifies the order of the results. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## **listPasswordViewRequestSummary**

Use the listPasswordViewRequestSummary command to return a list of password view requests.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=listPasswordViewRequestSummary
```

### **Parameters**

You can use the following parameters with the searchPasswordViewRequest command.

#### **TIP**

Any parameter that contains a space must be enclosed between quotation marks.

### ***PasswordViewRequest.requestorID***

Filter results for specified requestorID

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestorNameID***

Filter results for specified requestorNameID

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.approverID**

Filter results for specified approverID

Required	Default Value	Valid Values
no	N/A	Integer

**PasswordViewRequest.approverNameID**

Filter results for specified approverNameID (for approved password view requests).

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.status**

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checkin/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

**PasswordViewRequest.targetAccountID**

Filter results for specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

**PasswordViewRequest.targetAccountUserName**

Filter results for specified target account user name.

Required	Default Value	Valid Values
no	N/A	String

**PasswordViewRequest.policyApproverID**

Filter results for specified specified policy approver ID (for unapproved password view requests).

Required	Default Value	Valid Values
no	N/A	Integer

**PasswordViewRequest.policyApproverNameID**

Filter results for specified policy approver name ID (for unapproved password view requests).

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.ssoType***

Filter results the specified SSO type.

Required	Default Value	Valid Values
no	N/A	"Browser", "RDP", "SSH", "VNC", "AWSAPI", "Telnet", "Other"

### ***Page.Number***

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

### ***Page.Size***

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.requestorID, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### ***Sort.Direction***

Sort.Direction specifies the order of the results. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## **listRequestServer**

Use the listRequestServer command to retrieve a detailed listing of all registered request servers (Credential Manager clients) or those that match the specified search criteria.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=listRequestServer
```

```
RequestServer.hostName=myhostname.mydomain.com RequestServer.active=true
```

## Parameters

### **RequestServer.ID**

Filter results for the specified request server ID.

Required	Default Value	Valid Values
no	N/A	Numeric

### **RequestServer.hostName**

Filter results for request server host names that contain the specified value.

Required	Default Value	Valid Values
no	N/A	String

### **RequestServer.exactHostName**

Filter results for request server host names that exactly match the specified value.

Required	Default Value	Valid Values
yes	N/A	String

### **RequestServer.deviceName**

Filter results for request server device names that contain the specified value.

Required	Default Value	Valid Values
no	Same as host name.	String

### **RequestServer.exactDeviceName**

Filter results for a request server device name that exactly match the specified value

Required	Default Value	Valid Values
no	N/A	String

### **RequestServer.ipAddress**

Filter results for request servers with an IP address that contains the specified value.

Required	Default Value	Valid Values
no	N/A	String

### **RequestServer.exactIpAddress**

Filter results for a request server with an IP address that exactly matches the specified value.

Required	Default Value	Valid Values
no	N/A	String



**RequestServer.clientVersion**

Filter results for request servers with a client version that contains the specified value.

Required	Default Value	Valid Values
no	N/A	String

**RequestServer.active**

Set RequestServer.active=true to filter results for request servers that have the active flag set to true. Set RequestServer.active=false to filter results for request servers that have the active flag set to false..

Required	Default Value	Valid Values
no	false	true, false

**RequestServer.actionRequired**

Set RequestServer.actionRequired=true to filter results for request servers that have the action required flag set to true. Set RequestServer.actionRequired=false to filter results for request servers that have the actionRequired flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**Page.Number**

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

**Page.Size**

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

**Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	RequestServer.hostName	RequestServer.ID, RequestServer.hostName

**Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## listRequestServerDefaults

Use the listRequestServerDefaults command to retrieve a list of Request Server defaults from the Privileged Access Manager Credential Manager datastore.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin
cmdName=listRequestServerDefaults
```

### Parameters

#### RequestServerDefaults.ipAddress

The ip filter to apply to search.

Required	Default Value	Valid Values
no	N/A	String

#### RequestServerDefaults.type

The type filter to apply to search.

Required	Default Value	Valid Values
no		CLIENT, AGENT

## listUserAuthorization

Use the listUserAuthorization command to list user authorization mappings.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=listUserAuthorization
SecretAlias.name=test
```

### Parameters

#### UserAuthorization.ID

ID of the userAuthorization.

Required	Default Value	Valid Values
no	N/A	Numeric

#### TargetAlias.name

The name of the target alias.

Required	Default Value	Valid Values
no	N/A	String

#### TargetGroup.name

The name of the target group.

Required	Default Value	Valid Values
no	N/A	String

### **SecretAlias.name**

The name of the secret alias.

Required	Default Value	Valid Values
no	N/A	String

### **SecretGroup.name**

The name of the secret group.

Required	Default Value	Valid Values
no	N/A	String

### **User.userID**

The user name of the Credential Manager user.

Required	Default Value	Valid Values
no	N/A	String

### **UserGroup.name**

The user group name.

Required	Default Value	Valid Values
no	N/A	String

## **renameUser**

Use the renameUser command to rename a Credential Manager user. This command creates a copy of an existing user with a new name, and deletes the old user.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=renameUser
  User.userID=demo User.password=demo123$

User.newUserID=demo2
```

## **Parameters**

### **User.userID**

The user name of the Credential Manager user to be renamed.

Required	Default Value	Valid Values
yes	N/A	String

### **User.newUserID**

The user name of the Credential Manager user to be created.

Required	Default Value	Valid Values
yes	N/A	String

### **User.gkUserId**

The user ID to be associated with this user. If not specified, the existing value will be preserved.

Required	Default Value	Valid Values
optional (Credential Manager mode), rejected (PA mode)	N/A	Integer

## **resetClientCache**

The resetClientCache command informs all active clients that their caches of saved passwords should be reset. Use resetClientCache to reset all client caches.

### **WARNING**

We strongly recommend that you contact Broadcom Support before using this command.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=resetClientCache
```

## **resetDBHash**

Use the resetDBHash command to reset the database hash for an object. You can specify the types of objects as a comma separated list using the objectClass parameter.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=resetDBHash
objectClass=c.cw.m.ts
```

### **Parameter**

#### ***objectClass***

Required	Default	Value
No	c.cw.m.ts	

## resetGroupCache

Use the resetGroupCache command to refresh the group cache for all groups, or a single group. This command is asynchronous.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=resetGroupCache
Group.name=test_target_group
```

### Parameters

#### Group.name

Name of the group you wish to update in the group cache.

Required	Default Value	Valid Values
No. If not specified, all groups will be reset.	N/A	Numeric. This value must match the group ID registered in Credential Manager.

## searchAgent

Use the searchAgent command to retrieve a detailed listing of all the Windows Proxies registered in Credential Manager.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchAgent
```

### Parameters

#### Agent.ID

Filter results for the specified Agent.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

#### Agent.hostName

Filter results based on the Agent.hostName specified.

Required	Default Value	Valid Values
no	N/A	String

#### Agent.ipAddress

Filter results based on the Agent.ipAddress specified.

Required	Default Value	Valid Values
no	N/A	String

**Agent.deviceName**

Filter results based on the Agent.deviceName specified.

Required	Default Value	Valid Values
no	N/A	String

**Agent.clientVersion**

Filter results based on the Agent.clientVersion specified.

Required	Default Value	Valid Values
no	N/A	String

**Agent.active**

Set Agent.active=true to filter results for active agents. Set Agent.active=false to filter results for inactive agents.

Required	Default Value	Valid Values
no	N/A	true, false

**Agent.actionRequired**

Set Agent.actionRequired=true to filter results for agents with the actionRequired flag set to true. Set Agent.actionRequired=false to filter results for agents with the actionRequired flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

**Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

**Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	RequestServer.hostName	RequestServer.ID, RequestServer.hostName

**Sort.Direction**

Set Sort.Direction=asc to have the results presented in ascending order. Set Sort.Direction=desc to have the results presented in descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

**searchAuthorization**

Use the searchAuthorization command to retrieve a detailed listing of authorization mappings registered in Credential Manager, which match the provided search criteria. When no search criteria are listed all authorization mappings are returned.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchAuthorization
Authorization.checkExecutionID=true
```

**Parameters****Authorization.executionUser**

Filter results for specified authorization execution user.

Required	Default Value	Valid Values
no	N/A	N/A

**Authorization.checkExecutionID**

Set Authorization.checkExecutionID=true to filter results for authorization mappings that have the check execution ID flag set to true. Set Authorization.checkExecutionID=false to filter results for script authorizations. that have the check execution ID flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**Authorization.checkPath**

Set Authorization.checkPath=true to filter results for authorization mappings that have the check execution path flag set to true. Set Authorization.checkPath=false to filter results for authorization mappings that have the check execution path flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**Authorization.checkFilePath**

Set Authorization.checkFilePath=true to filter results for authorization mappings that have the check file path flag set to true. Set Authorization.checkFilePath=false to filter results for authorization mappings that have the check file path flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

#### **Authorization.checkScriptHash**

Set Authorization.checkScriptHash=true to filter results for authorization mappings that have the check script hash flag set to true. Set Authorization.checkScriptHash=false to filter results for authorization mappings that have the check script hash flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

#### **Authorization.ID**

Filter results based on Authorization.ID specified.

Required	Default Value	Valid Values
no	N/A	Numeric.

#### **RequestServer.ID**

Filter results based on the RequestServer.ID specified.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchRequestServer to retrieve RequestServer.ID.

#### **RequestScript.ID**

Filter results based on the RequestScript.ID specified.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchRequestScript to retrieve RequestScript.ID.

#### **TargetAlias.ID**

Filter results based on the TargetAlias.ID specified.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetAlias to retrieve the TargetAlias.ID.

#### **Authorization.targetGroupID**



Filter results based on the targetGroupId specified.

Required	Default Value	Valid Values
no	N/A	Numeric

### **Authorization.requestGroupId**

Filter results based on the requestGroupId specified.

Required	Default Value	Valid Values
no	N/A	Numeric

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	TargetAlias.ID	Authorization.executionUser, Authorization.checkExecutionID, Authorization.checkPath, Authorization.checkFilePath, Authorization.checkScriptHash, Authorization.ID, RequestServer.ID, RequestScript.ID, TargetAlias.ID, Authorization.targetGroupId, Authorization.requestGroupId

### **Sort.Direction**

Set Sort.Direction=asc to have the results presented in ascending order. Set Sort.Direction=desc to have the results presented in descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## searchFilter

Use the searchFilter command to retrieve a detailed listing of filters which match the provided search criteria. When no search criteria is listed, all registered filters are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchFilter
```

## Parameters

### Filter.ID

Filter results for the specified filter.

Required	Default Value	Valid Values
no	N/A	Numeric

### Group.ID

Filter results for the unique identifier of a request or target group.

Required	Default Value	Valid Values
no	N/A	Numeric

### Filter.attribute

The filter attribute. For a list of attributes, see [Set up Command Filters](#).

Required	Default Value	Valid Values
no	N/A	String

### Filter.type

Filter results for the specified filter type.

Required	Default Value	Valid Values
no	N/A	equals, beginswith, contains, endswith

### Filter.expression

Filter results for the specified filter expression.

Required	Default Value	Valid Values
no	N/A	String

### Filter.objectClassId

Filter results for the specified object class ID.

Required	Default Value	Valid Values
no	N/A	String

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	TargetAlias.ID	Group.ID, Filter.ID, Filter.attribute, Filter.type, Filter.expression, Filter.objectClassId

### **Sort.Direction**

Set Sort.Direction=asc to have the results presented in ascending order. Set Sort.Direction=desc to have the results presented in descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## **searchGroup**

Use the searchGroup command to retrieve a list of target groups or request groups within Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchGroup
```

### **Parameters**

#### **Group.ID**

Filter results for the specified Group.ID.

Required	Default Value	Valid Values
no	N/A	String

### **Group.name**

Filter results for groups matching the specified name.

Required	Default Value	Valid Values
no	N/A	String

### **Group.description**

Filter results for groups matching the specified description.

Required	Default Value	Valid Values
no	N/A	String

### **Group.type**

Filter results for groups with the specified group type.

Required	Default Value	Valid Values
no	N/A	target, requestor

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	Group.name	Group.ID, Group.name, Group.description, Group.type, Group.dynamic

### **Sort.Direction**

Set Sort.Direction=asc to have the results presented in ascending order. Set Sort.Direction=desc to have the results presented in descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

### **Group.isSecretType**

Use Group.isSecretType to search for secret groups.

Required	Default Value	Valid Values
no	false	string

## **searchPasswordPolicy**

Use the searchPasswordPolicy command to retrieve a detailed list of all the Password Composition policies that match the provided search criteria. If no search criteria are specified then all SSH Key Pair policies are returned.

### **Example**

```
capam_command capam=capamServer UserInputException cmdName=searchPasswordPolicy
```

### **Parameters**

#### **PasswordPolicy.name**

Filter results for specified policy name.

Required	Default Value	Valid Values
No	N/A	String

#### **PasswordPolicy.description**

Filter results for policy descriptions that contain the specified value.

Required	Default Value	Valid Values
No	N/A	String

#### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works with Page.Size.

Required	Default Value	Valid Values
No	1	Numeric

#### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
No	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
No	PasswordPolicy.name	PasswordPolicy.name, PasswordPolicy.description

### **Sort.Direction**

Sort.Direction determines the order in which results are displayed. Select **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
No	asc	asc, desc

## **searchPasswordViewPolicy**

Use the searchPasswordViewPolicy command to retrieve a list of all password view policies that match the search criteria. When no search criteria are listed, all password view policies are returned.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=searchPasswordViewPolicy PasswordViewPolicy.name=restrictedAccounts
```

### **Parameters**

#### **PasswordViewPolicy.name**

The name of the password view policy.

Required	Default Value	Valid Values
no	N/A	Any text string

#### **PasswordViewPolicy.description**

The description of the password view policy.

Required	Default Value	Valid Values
no	N/A	Any text string

#### **PasswordViewRequest.connectionTimeout**

Filter results for requests with connection idle timeouts greater than or equal to the specified value. (Useful for identifying extended timeout requests.)

Required	Default Value	Valid Values
no	N/A	Numeric

### **Page.Number**

Specifies which page to return when the results are divided among multiple pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewPolicy.name	PasswordViewPolicy.name, PasswordViewPolicy.description

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## **searchPasswordViewRequest**

Use the searchPasswordViewRequest command to list all password view requests. This information is useful for reporting purposes. The approver is the user executing the command.

### **NOTE**

Use the [searchPasswordViewRequestByApprover](#) command to see all password view requests that can be or have been approved by the user issuing the command. Use the [searchPasswordViewRequestByRequestor](#) command to see all password view requests made by the user issuing the command.

### **Example**

The following example shows how to use the searchPasswordViewRequest command. This example is for UNIX/Linux.

```
capam_command cmdName=searchPasswordViewRequest capam=uspam12.ca.com
adminUserID=admin adminPassword=test
```

```
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
```

```
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

## Parameters

### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checkin/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

### ***PasswordViewRequest.connectionTimeout***

Filter results for requests with connection idle timeouts greater than or equal to the specified value (in minutes). (Useful for identifying extended timeout requests.)

Required	Default Value	Valid Values
no	N/A	Positive integer

### ***PasswordViewRequest.targetAccountID***

Filter results for the specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.RequestorID***

Filter results for the specified requestor ID.

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.ApproverID***

Filter results for the specified requestor ID.

Required	Default Value	Valid Values
no	N/A	Integer

### ***PasswordViewRequest.requestPeriodStart***



Filter results are based on a specified start time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any view request that is active within a specified start and end time. The results can include view requests that start before the specified start time, as long as the request is active. To understand which view requests are returned, see [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodEnd parameter. If you do not specify a start time, the start time defaults to the time of the first entry in the Credential Manager database.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodStart=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***PasswordViewRequest.requestPeriodEnd***

Filter results are based on a specified end time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any password view request that is active within a specified start and end time. The results can include view requests that end after the specified end time, as long as the request is active. To understand which view requests are returned, see the [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodStart parameter. However, if you do not specify an end time, the time defaults to when the CLI command is submitted to the appliance.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodEnd=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***Example: View Requests Returned in a Specified Time Period***

This PasswordViewRequest.requestPeriodStart and PasswordViewRequest.requestPeriodEnd parameters work together to define a time period for returned view requests.

The following parameter example shows a start time of 14:10 and an end time of 15:00:

```
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
```

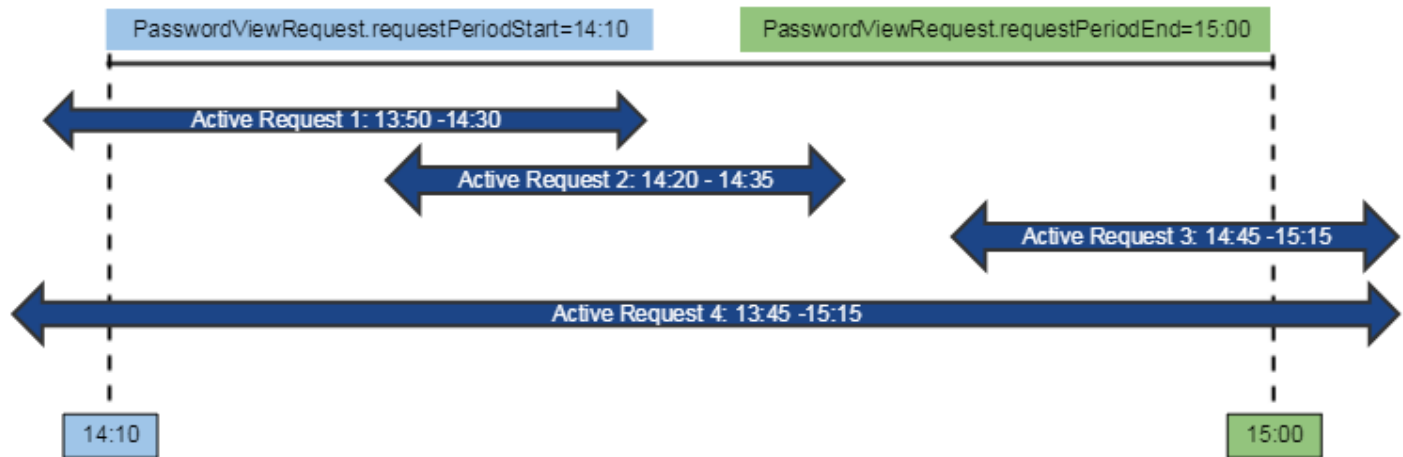
```
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

Within the 14:10 to 15:00 time frame, the results include the following active requests:

Active Request Start	Active Request End
Starts at 13:50	Ends at 14:30
Starts at 14:20	Ends at 14:35
Starts at 14:45	Ends at 15:15
Starts at 13:45	Ends at 15:15

These results are illustrated in the following diagram:

**Figure 66: searchPasswordViewRequest Example**



### **Page.Number**

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

### **Page.Size**

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### **Sort.Direction**

Set Sort.Direction=asc to present the results in ascending order. Set Sort.Direction=desc to present the results in descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## searchPasswordViewRequestByApprover

Use the searchPasswordViewRequestByApprover command to list the password view requests for a particular approver. This information is useful for reporting purposes. The approver is the user executing the command.

### Example

The following example shows how to use the searchPasswordViewRequestByApprover command. This example is for UNIX/Linux.

```
capam_command cmdName=searchPasswordViewRequestByApprover capam=uspm12.ca.com
adminUserID=admin adminPassword=test
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

### Parameters

#### ***PasswordViewRequest.requestorID***

Filter results for specified requestorID

Required	Default Value	Valid Values
no	N/A	Integer

#### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checkin/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

#### ***PasswordViewRequest.connectionTimeout***

Filter results for requests with connection idle timeouts greater than or equal to the specified value (in minutes). (Useful for identifying extended timeout requests.)

Required	Default Value	Valid Values
no	N/A	Positive integer

#### ***PasswordViewRequest.targetAccountID***

Filter results for specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

#### ***PasswordViewRequest.requestPeriodStart***

Filter results are based on a specified start time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any view request that is active within a specified start and end time. The results can include view requests that start before the specified start time, as long as the request is active. To understand which view requests are returned, see [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodEnd parameter. If you do not specify a start time, the start time defaults to the time of the first entry in the Credential Manager database.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodStart=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***PasswordViewRequest.requestPeriodEnd***

Filter results are based on a specified end time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any password view request that is active within a specified start and end time. The results can include view requests that end after the specified end time, as long as the request is active. To understand which view requests are returned, see the [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodStart parameter. However, if you do not specify an end time, the time defaults to when the CLI command is submitted to the appliance.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodEnd=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***Example: View Requests Returned in a Specified Time Period***

This PasswordViewRequest.requestPeriodStart and PasswordViewRequest.requestPeriodEnd parameters work together to define a time period for returned view requests.

The following parameter example shows a start time of 14:10 and an end time of 15:00:

```
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
```

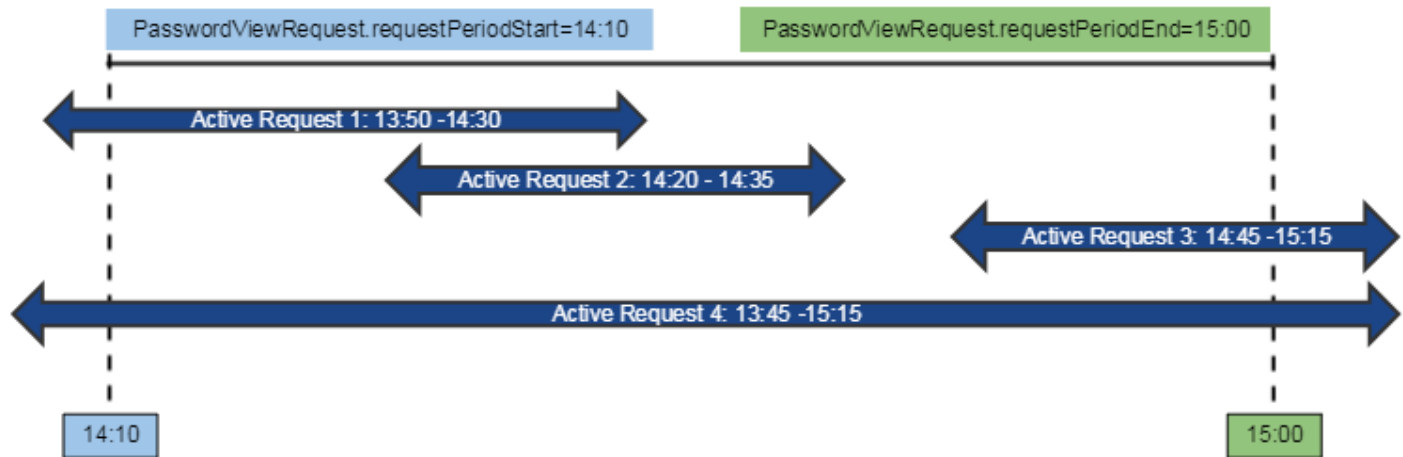
```
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

Within the 14:10 to 15:00 time frame, the results include the following active requests:

Active Request Start	Active Request End
Starts at 13:50	Ends at 14:30
Starts at 14:20	Ends at 14:35
Starts at 14:45	Ends at 15:15
Starts at 13:45	Ends at 15:15

These results are illustrated in the following picture:

**Figure 67: searchPasswordViewRequestByApprover Example**



### Page.Number

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

### Page.Size

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### Sort.Property

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status, PasswordViewRequest.approverID, PasswordViewRequest.targetAccountID

### Sort.Direction

Set Sort.Direction=asc to present the results in ascending order. Set Sort.Direction=desc to present the results in descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## searchPasswordViewRequestByRequestor

Use the searchPasswordViewRequestByRequestor command to list the password view requests for a particular requestor. This information is useful for reporting purposes. The requestor is the user making the view request.

### Example

The following example shows how to use the searchPasswordViewRequestByRequestor command. This example is for UNIX/Linux.

```
capam_command cmdName=searchPasswordViewRequestByRequestor capam=uspsam12.ca.com
adminUserID=admin adminPassword=test
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

### Parameters

#### ***PasswordViewRequest.approverID***

Filter results for specified approverID.

Required	Default Value	Valid Values
no	N/A	Integer.

#### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2), "pending" (or 3), "expiredapproved" (or 6), expiredpending (or 8) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10), "retrospectivePending" (or 11) <b>Checkin/checkout:</b> "checkout" (or 4), "checkedin" (or 5)

#### ***PasswordViewRequest.connectionTimeout***

Filter results for requests with connection idle timeouts greater than or equal to the specified value (in minutes). (Useful for identifying extended timeout requests.)

Required	Default Value	Valid Values
no	N/A	Positive integer

#### ***PasswordViewRequest.targetAccountID***

Filter results for specified target account ID.

Required	Default Value	Valid Values
no	N/A	Integer

#### ***PasswordViewRequest.isCheckedOut***

Filter results for accounts that are checked out.

Required	Default Value	Valid Values
no	N/A	"true" or "false"

### ***PasswordViewRequest.requestPeriodStart***

Filter results are based on a specified start time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any view request that is active within a specified start and end time. The results can include view requests that start before the specified start time, as long as the request is active. To understand which view requests are returned, see [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodEnd parameter. If you do not specify a start time, the start time defaults to the time of the first entry in the Credential Manager database.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodStart=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***PasswordViewRequest.requestPeriodEnd***

Filter results are based on a specified end time.

Required	Default Value	Valid Values
no	N/A	N/A

The CLI includes any password view request that is active within a specified start and end time. The results can include view requests that end after the specified end time, as long as the request is active. To understand which view requests are returned, see the [Example: View Requests Returned in a Specified Time Period](#).

This parameter is intended to work with the PasswordViewRequest.requestPeriodStart parameter. However, if you do not specify an end time, the time defaults to when the CLI command is submitted to the appliance.

Parameter syntax:

```
"PasswordViewRequest.requestPeriodEnd=YYYY-MM-DD HH:MM"
```

The date format must be: YYYY-MM-DD HH:MM

### ***Example: View Requests Returned in a Specified Time Period***

This PasswordViewRequest.requestPeriodStart and PasswordViewRequest.requestPeriodEnd parameters work together to define a time period for returned view requests.

The following parameter example shows a start time of 14:10 and an end time of 15:00:

```
"PasswordViewRequest.requestPeriodStart=2018-02-22 14:10"
```

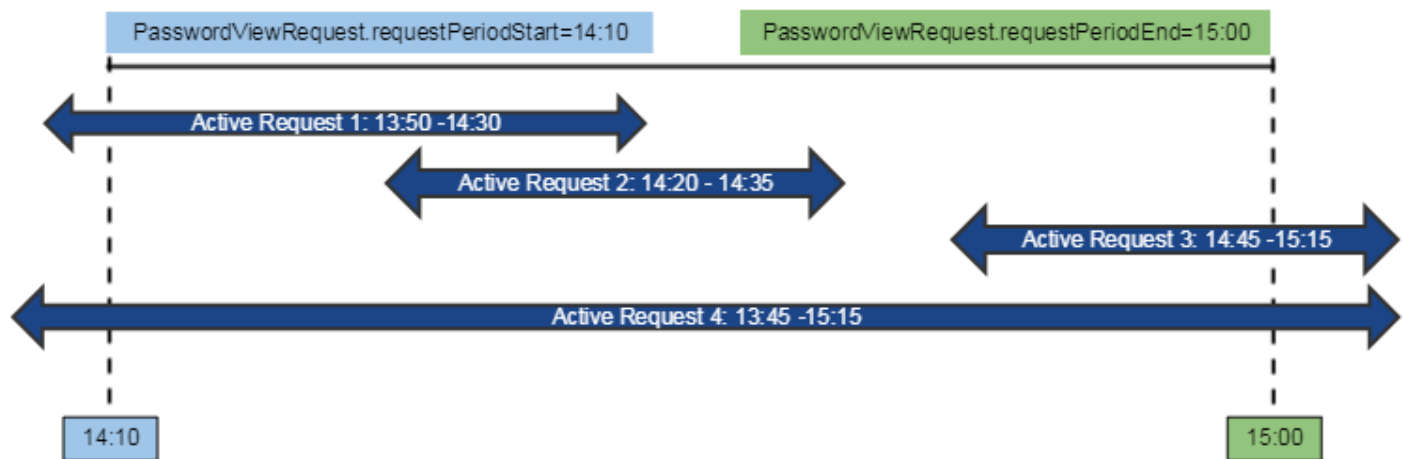
```
"PasswordViewRequest.requestPeriodEnd=2018-02-22 15:00"
```

Within the 14:10 to 15:00 time frame, the results include the following active requests:

Active Request Start	Active Request End
Starts at 13:50	Ends at 14:30
Starts at 14:20	Ends at 14:35
Starts at 14:45	Ends at 15:15
Starts at 13:45	Ends at 15:15

These results are illustrated in the following picture:

**Figure 68: searchPasswordViewRequestByRequestor Example**



### **Page.Number**

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

### **Page.Size**

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	PasswordViewRequest.status	PasswordViewRequest.status PasswordViewRequest.approverID PasswordViewRequest.targetAccountID

### **Sort.Direction**



Sort.Direction determines the sort order. Select **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	desc	asc, desc

## searchRequestScript

Use the searchRequestScript command to retrieve a detailed list of requesting applications that are registered with Credential Manager. The resulting list matches the search criteria. If no search criteria are specified, all registered requesting applications are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchRequestScript
RequestScript.name=example.pl
```

### Parameters

#### RequestServer.ID

Filter results for specified RequestServer.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchRequestServer to retrieve the RequestServer.ID

#### RequestScript.name

Filter results for specified request script name.

Required	Default Value	Valid Values
no	N/A	String

#### RequestScript.ID

Filter results for specified RequestScript.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

#### RequestScript.filePath

Filter results for file paths that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

#### RequestScript.executionPath

Filter results for execution paths that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	RequestScript.name	RequestServer.ID, RequestScript.name, RequestScript.ID, RequestScript.filePath, RequestScript.executionPath

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## **searchRequestServer**

Use the searchRequestServer command to retrieve a detailed list of request servers (Credential Manager clients) that are registered with Credential Manager. The resulting list matches the search criteria. If no search criteria is provided, all registered request servers are returned.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchRequestServer
RequestServer.hostName=mydomain
```

**Parameters****RequestServer.ID**

Filter results for specified RequestServer.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

**RequestServer.hostName**

Filter results for request server host names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

**RequestServer.deviceName**

Filter results for request server device names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

**RequestServer.ipAddress**

Filter results for IP address that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

**RequestServer.clientVersion**

Filter results for request server client version that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

**RequestServer.active**

Set RequestServer.active=true to filter results for request servers that have the active flag set to true. Set RequestServer.active=false to filter results for request servers that have the active flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**RequestServer.actionRequired**

Set RequestServer.actionRequired=true to filter results for request servers that have the action required flag set to true. Set RequestServer.actionRequired=false to filter results for request servers that have the actionRequired flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

**Page.Number**

List all request servers within the specified page.

Required	Default Value	Valid Values
no	1	N/A

**Page.Size**

Specify the size of each page.

Required	Default Value	Valid Values
no	10000	N/A

**Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	RequestServer.hostName	RequestServer.ID, RequestServer.hostName

**Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

**searchRole**

Use the searchRole command to retrieve roles from Credential Manager.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchRole
```

**Parameters****Role.ID**

Filter results for specified Role.ID.

Required	Default Value	Valid Values
yes	N/A	Numeric

**Role.name**

Filter results based on the Role.name specified.

Required	Default Value	Valid Values
yes	N/A	String

### **Role.description**

Filter results based on the Role.description specified.

Required	Default Value	Valid Values
no	N/A	String

### **Page.Number**

List all roles within the specified page.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	Role.name	Role.ID, Role.name, Role.description

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify asc for ascending order or desc for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## **searchSite**

Use the searchSite command to retrieve an XML list of all sites registered with Credential Manager. This command takes no parameters.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchSite
```

## searchSSHKeyPairPolicy

Use this command to retrieve a detailed list of all the SSH key pair policies that match the search criteria. If no search criteria are specified, all SSH Key Pair policies are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=searchSSHKeyPairPolicy
```

### Parameters

#### ***SSHKeyPairPolicy.name***

Filter results for specified policy name.

Required	Default Value	Valid Values
No	N/A	String

#### ***SSHKeyPairPolicy.description***

Filter results for policy descriptions that contain the specified value.

Required	Default Value	Valid Values
No	N/A	String

#### ***Page.Number***

Specifies which page to return when the results are divided among multiple a pages. This parameter works with Page.Size.

Required	Default Value	Valid Values
No	1	Numeric

#### ***Page.Size***

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
No	10000	Numeric

#### ***Sort.Property***

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
No	SSHKeyPairPolicy.name	SSHKeyPairPolicy.name, SSHKeyPairPolicy.description

#### ***Sort.Direction***

Sort.Direction specifies the order in which results are displayed. Specify asc for ascending order or desc for descending order.

Required	Default Value	Valid Values
No	asc	asc, desc

## searchTargetAccount

Use the searchTargetAccount command to retrieve an XML listing of all target accounts that match the search criteria. If no search criteria are listed, all target accounts are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchTargetAccount
TargetAccount.userName=root
```

### Parameters

#### TargetAccount.ID

Filter results for specified TargetAccount.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

#### TargetApplication.ID

Filter results for specified TargetApplication.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetApplication to retrieve the TargetApplication.ID

#### TargetServer.ID

Filter results for specified TargetServer.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetServer to retrieve the TargetServer.ID

#### TargetApplication.name

Filter results for specified target application name.

Required	Default Value	Valid Values
no	N/A	String

#### TargetApplication.type

Filter results for specified target application type.

Required	Default Value	Valid Values
no	N/A	String

### **TargetAccount.userName**

Filter results for target account user names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **TargetAccount.accessType**

Filter results for target account access types that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **TargetAccount.cacheAllow (Deprecated)**

Set TargetAccount.cacheAllow=true to filter results for target accounts that have the cache allow flag set to true. Set TargetAccount.cacheAllow=false to filter results for target accounts that have the cache allow flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

### **TargetAccount.cacheBehavior**

Set this parameter to **useCacheFirst** to cache the account credentials in the Credential Manager client and used first. Set the parameter to **useServerFirst** to cache the account credentials in the Credential Manager client but the server is contacted first. To not cache the account credentials, set this parameter to **noCache**.

Required	Default Value	Valid Values
no	useCacheFirst	useCacheFirst, useServerFirst, noCache

### **TargetAccount.cacheDuration**

Filter results for specified cache duration value.

Required	Default Value	Valid Values
no	N/A	Numeric

### **TargetAccount.privileged**

Set this parameter to **true** to filter results for target accounts with the privileged flag set to true. Select **false** to filter results for target accounts with the privileged flag set to false (A2A accounts).

Required	Default Value	Valid Values
no	N/A	true, false

### **TargetAccount.synchronize**



Set this parameter to **true** to filter results for target accounts with the synchronize flag set to true. Select **false** to filter results for target accounts with the synchronize flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

### **TargetAccount.passwordVerified**

Set this parameter to **true** to filter results for target accounts with the password verified flag set to true. Select **false** to filter results for target accounts with the password verified flag set to false.

Required	Default Value	Valid Values
no	N/A	true, false

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specified which field to use for sorting the result.

Required	Default Value	Valid Values
no	TargetAccount.ID	TargetAccount.ID, TargetApplication.ID, TargetApplication.name, TargetApplication.type, TargetAccount.userName, TargetAccount.accessType, TargetAccount.cacheAllow, TargetAccount.cacheDuration, TargetAccount.privileged, TargetAccount.synchronize, TargetAccount.passwordVerified

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify asc for ascending order or desc for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## searchTargetAlias

Use the searchTargetAlias command to retrieve an XML list of all target aliases that match the search criteria. If no search criteria are specified, all target aliases are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchTargetAlias
TargetAlias.name=test
```

### Parameters

#### TargetAlias.name

Filter results for target alias names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

#### TargetAccount.ID

Filter results for specified TargetAccount.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetAccount to retrieve the TargetAccount.ID

#### TargetAlias.ID

Filter results for specified TargetAlias.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

#### TargetServer.hostName

Filter results for target server host names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

#### TargetApplication.name

Filter results for target application names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

#### TargetAccount.userName

Filter results for target account user names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	TargetAlias.name	TargetAlias.name, TargetAccount.ID, TargetAlias.ID

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## **searchTargetApplication**

Use the searchTargetApplication command to retrieve an XML listing of all target applications that match the search criteria. If no search criteria are specified, all target applications are returned.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=searchTargetApplication TargetApplication.type=oracle
```

### **Parameters**

#### **TargetApplication.ID**

Filter results for specified TargetApplication.ID.

Required	Default Value	Valid Values
no	N/A	Numeric

### **TargetServer.ID**

Filter results for specified TargetServer.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetServer to retrieve the TargetServer.ID

### **TargetApplication.name**

Filter results for target application names that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **TargetApplication.type**

Filter results for target application types that contain the value specified.

Required	Default Value	Valid Values
no	N/A	String

### **Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

### **Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

### **Sort.Property**

Use Sort.Property to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	TargetApplication.name	TargetApplication.ID, TargetServer.ID, TargetApplication.name, TargetApplication.type

### **Sort.Direction**

Sort.Direction specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

## searchTargetServer

Use the `searchTargetServer` command to retrieve an XML list of all target servers that match the search criteria. If no search criteria are specified, all target servers are returned.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=searchTargetServer
TargetServer.hostName=mydomain
```

## Parameters

### ts.TargetServer.ID

Filter results for a target server ID that contain the specified value. Add the table alias `ts` as a prefix.

```
capam_command capam=capamServer adminUserID=admin adminPassword=password
cmdName=searchTargetServer ts.TargetServer.ID=1000
```

Required	Default Value	Valid Values
no	N/A	String

### TargetServer.hostName

Filter results for target server host names that contain the specified value.

Required	Default Value	Valid Values
no	N/A	String

### TargetServer.ipAddress

Filter results for IP addresses that contain the specified value.

Required	Default Value	Valid Values
no	N/A	String

### TargetServer.deviceName

Filter results for target server device names that contain the specified value.

Required	Default Value	Valid Values
no	N/A	String

**Page.Number**

Specify which page to return when the results are divided among multiple pages. This parameter works with `Page.Size`.

Required	Default Value	Valid Values
no	1	Numeric

**Page.Size**

Specify the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

**Sort.Property**

Use `Sort.Property` to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	<code>TargetServer.hostName</code>	<code>TargetServer.hostName</code> , <code>TargetServer.ipAddress</code>

**Sort.Direction**

`Sort.Direction` specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

**searchUser**

Use the `searchUser` command to retrieve a list of Credential Manager users from the Credential Manager database.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchUser
  UserGroup.ID=4 User.authenticationType=CSPM
```

```
User.status=ACTIVE User.firstName=Demo User.lastName=User
```

**Parameters****UserGroup.ID**

Filter results for users belonging to the specified user group.

Required	Default Value	Valid Values
no	N/A	Numeric. Use <code>searchUserGroup</code> to retrieve the <code>UserGroup.ID</code>

**User.authenticationType**

Filter results on user authenticationType.

Required	Default Value	Valid Values
no	N/A	String

**User.status**

Filter results on user status.

Required	Default Value	Valid Values
no	N/A	ACTIVE

**User.firstName**

Filter results on user first name.

Required	Default Value	Valid Values
no	N/A	String

**User.lastName**

Filter results on user last name.

Required	Default Value	Valid Values
no	N/A	String

**UserGroup.includeInheritedUsers**

Use this parameter with the UserGroup.ID parameter alone. It causes the command to return all users who are direct members of the specified CM user group as well as those users who inherit the specified CM user group from some AM user group. All other filters such as User.firstName, User.lastName, are ignored if this filter is used.

Required	Default Value	Valid Values
no	false	Boolean (true/false)

**Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

**searchUserGroup**

Use the searchUserGroup command to retrieve a list of user groups from the Credential Manager database. If an individual user is specified, then only the groups in which that user belongs are displayed.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=searchUserGroup UserGroup.ID=1
```

**Parameters****UserGroup.ID**

Filter results for user groups matching the specified ID.

Required	Default Value	Valid Values
no	N/A	String

**UserGroup.name**

Filter results for user groups matching the specified name.

Required	Default Value	Valid Values
no	N/A	String

**UserGroup.description**

Filter results for user groups matching the specified description.

Required	Default Value	Valid Values
no	N/A	String

**UserGroup.userID**

Filter results for user groups in which the specified user belongs.

Required	Default Value	Valid Values
no	N/A	String

**Page.Number**

Specifies which page to return when the results are divided among multiple a pages. This parameter works in conjunction with Page.Size.

Required	Default Value	Valid Values
no	1	Numeric

**Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	10000	Numeric

**Sort.Property**



Use `Sort.Property` to specify which field to use for sorting the result.

Required	Default Value	Valid Values
no	UserGroup.name	UserGroup.ID, UserGroup.name, UserGroup.description, UserGroup.userID, UserGroup.amUserGroupID

### **Sort.Direction**

`Sort.Direction` specifies the order in which results are displayed. Specify **asc** for ascending order or **desc** for descending order.

Required	Default Value	Valid Values
no	asc	asc, desc

### **UserGroup.amUserGroupID**

`UserGroup.amUserGroupID` filters results for user groups in which the specified AM user group belongs.

Required	Default Value	Valid Values
no	N/A	Integer

### **UserGroup.includeInheritedCmGroups**

Use `UserGroup.includeInheritedCmGroups` with the `UserGroupID` parameter alone. It returns both direct and inherited CM user groups not a given user.

Required	Default Value	Valid Values
false	false	Boolean (true/false)

## **setDisasterRecoverySettings**

Use the `setDisasterRecoverySettings` command to enable or disable disaster recovery mode.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=setDisasterRecoverySettings enable=true
```

### **Parameters**

#### ***enable***

Set `enable=true` to enable the disaster recovery mode. Otherwise, set `enable=false` to disable it.

Required	Default Value	Valid Values
yes	false	true, false

## setInitProperty

Use the setInitProperty command to change the Credential Manager initialization property (database username and password) for DB2 databases. For all other databases, use the updateDBPassword command. This command can be executed at a secondary site.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=setInitProperty
propertyName=dbpassword propertyValue='12345'
```

### Parameters

#### propertyName

The property to set.

Required	Default Value	Valid Values
yes	N/A	dbpassword, dbusername, ddlpassword, ddlusername

#### propertyValue

String containing the property value.

Required	Default Value	Valid Values
yes	N/A	String. In UNIX, if special characters are included, the password must be enclosed in single quotes.

## setLocalProperty

Use the setLocalProperty command to set the site name of a primary or secondary site in a multi-site cluster. This command sets the site name in the site-local Credential Manager database.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=setLocalProperty
propertyName=sitename propertyValues=mySiteName
```

### Parameters

#### propertyName

The property to set.

Required	Default Value	Valid Values
yes	N/A	sitename

#### propertyValues

String containing the property value.

Required	Default Value	Valid Values
yes	N/A	String

## setPasswordViewReasons

Use the setPasswordViewReasons command to customize the reasons that a user can select for viewing a target account password.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=setPasswordViewReasons

reasons="System failure|System recovery|System update|Scheduled maintenance|
Other"
```

### Parameters

#### reasons

The list of reasons is delimited by the pipe character, (|). For UNIX, the list must be enclosed in quotes.

Required	Default Value	Valid Values
yes	N/A	String

## setPasswordViewRequestDeleteInterval

Use the setPasswordViewRequestDeleteInterval command to set the number of days to keep a password view request before they are deleted.

### Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=SetPasswordViewRequestDeleteInterval deleteIntervalDays=30
```

### Parameters

#### deleteIntervalDays

The number of days to keep password view requests

Required	Default Value	Valid Values
yes	N/A	Numeric

## setReportRowLimit

Use the setReportRowLimit command to set the maximum number of entries that are displayed in a report.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=setReportRowLimit
rowLimit=10000
```

### Parameters

#### *rowLimit*

Specifies the maximum number of entries displayed by each report.

Required	Default Value	Valid Values
yes	N/A	Numeric

## setSystemProperty

Use the setSystemProperty command to set a Credential Manager system property.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=setSystemProperty
propertyName=lunaPassword

propertyValues='p@ssw0rd!' encryptValue=true
```

### Parameters

#### *propertyName*

The property to update or if it does not exist, to insert the property.

Required	Default Value	Valid Values
yes	N/A	String

#### *propertyValues*

String containing the property value.

Required	Default Value	Valid Values
yes	N/A	String

#### *encryptValue*

Set encryptValue to true to encrypt the propertyValues string. To leave the value unencrypted (in plain text), set encryptValue to false.

Required	Default Value	Valid Values
no	false	true, false

### ***propertyValueBlankAllowed***

Indicates that an empty propertyValue parameter is allowed.

Required	Default Value	Valid Values
no	false	true, false

### ***clientInactivityCheckHours***

This property is for use by CA Technologies Support to help debug customer issues. Do not change the default value.

Required	Default Value	Valid Values
no	30	

### ***eventsCountThresholdValue***

Used to set the threshold count of the unprocessed child events.

Required	Default Value	Valid Values
no	N/A	Integer

### ***eventProcessorPoolSize***

Sets the pool size of the event processor. If this property is not set, its default value is 10.

Required	Default Value	Valid Values
no	10	Integer

### ***targetAccountPasswordExpirationEnabled***

Set the property value to True to enable automatic updating of expired passwords.

Required	Default Value	Valid Values
no	false	true, false

### ***oneclickServerHost***

Credential Manager Primary Host name

Required	Default Value	Valid Values
no	N/A	Server name

### ***emailServerHost***

Host name of the mail server.

Required	Default Value	Valid Values
no	mail.yourdomain.com	true, false

### ***emailServerPort***

Port number the SMTP service listens

Required	Default Value	Valid Values
no	25	Port number

### ***emailTransportType***

Email transport type

Required	Default Value	Valid Values
no	smtp	smtp

### ***emailTargetAccountID***

ID of the target email account

Required	Default Value	Valid Values
no	N/A	account ID

### ***emailFromAddress***

The "From" address for emails.

Required	Default Value	Valid Values
no	N/A	view_requests@yourdomain.com

### ***emailRequestSubject***

Property for configuring the request email. This is an optional property.

Required	Default Value	Valid Values
no	Password View Request for target account @TargetAccount.getUserName@	N/A

### ***emailRequestBody***

Property for configuring the request email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email. A password view request has been submitted by user @User.getUserID@ to view the password for account @TargetAccount.getUserName@ of application @TargetApplication.getName@ on server @TargetServer.getHostName@. The password view request reason is @PasswordViewRequest.getReason@ (@PasswordViewRequest.getReasonDescription@). Please login to the CPA system and manage this request.	N/A

#### ***emailRequestStatusSubject***

Property for configuring the request status email. This is an optional property.

Required	Default Value	Valid Values
no	Password View Request Status for account @TargetAccount.getUserName@	N/A

#### ***emailRequestStatusBody***

Property for configuring the request status email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email. The status of your request to view password for the account @TargetAccount.getUserName@ of application @TargetApplication.getName@ in server @TargetServer.getHostName@, is: @PasswordViewRequest.getStatusString@.	N/A

#### ***emailPasswordViewSubject***

Property for configuring the password view email. This is an optional property.

Required	Default Value	Valid Values
no	Password of account @TargetAccount.getUserName@ has been accessed by @User.getUserID@	N/A

#### ***emailPasswordViewBody***

Property for configuring the password view email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email. The Password for the account @TargetAccount.getUserName@ of application @TargetApplication.getName@ on server @TargetServer.getHostName@ has been accessed by user @User.getUserId@.	N/A

#### ***emailPasswordViewRequestExpiredSubject***

Property for configuring the expired password view request email. This is an optional property.

Required	Default Value	Valid Values
no	Password View Request for account @TargetAccount.getUserName@ requested by @User.getUserId@ has expired	N/A

#### ***emailPasswordViewRequestExpiredBody***

Property for configuring the expired password view request email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email. The Password View Request for the account @TargetAccount.getUserName@ of application @TargetApplication.getName@ on server @TargetServer.getHostName@ requested by user @User.getUserId@ has expired.	N/A

#### ***emailOneClickPasswordApprovalSubject***



Property for configuring one click approval email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email.   A password view request has been submitted with the following details:  Requestor : @User.getUserID@ Requested Account: @TargetAccount.getUserName@ Requested Account Target Application Name: @TargetApplication.getName@ Requested Account Target Server: @TargetServer.getHostName@ Request Reason: @PasswordViewRequest.getReason@ (@PasswordViewRequest.getReasonDescription@) Start Date: @PasswordViewRequest.getStartDate@ End Date: @PasswordViewRequest.getEndDate@  <a href='@ApprovalURL@'>Click here to Approve this Request</a>  <a href='@DenialURL@'>Click here to Deny this Request</a>	N/A

#### ***emailOneClickPasswordApprovalBody***

Property for configuring one click approval email. This is an optional property.

Required	Default Value	Valid Values
no	Password View Request for target account @TargetAccount.getUserName@	N/A

#### ***emailReportResultSubject***

Property for configuring the report results email. This is an optional property.

Required	Default Value	Valid Values
no	Report results for @reportName@	N/A

#### ***emailReportResultBody***

Property for configuring the report results email. This is an optional property.

Required	Default Value	Valid Values
no	Do not reply to this email. The @reportName@ report has been run. The attached results encompass the period from @reportStartDate@ to @reportEndDate@.	N/A

#### ***reportAttachmentLimit***

Specifies the maximum size of a report email attachment, for example, 1 MB.

Required	Default Value	Notes	encryptValue
no	5 MB	Set an integer value in MB	False

### ***ViewPasswordReasons***

When a user wants to view a password, the reasons are shown in a drop-down list. Multiple reasons are delimited by the pipe (|) character, such as reason1|reason2.

Required	Default Value	Valid Values
no	N/A	Severity 1: Manual recovery from server outage Severity 1: Manual change due to potential password breach Severity 2: Password composition audit Severity 3: Application migration Severity 3: Pre-production application testing Other

### ***viewPasswordApprovalReasons***

Use to view password approval reason, the options are shown in a drop-down list.

Required	Default Value	Valid Values
no	N/A	Approve

### ***viewPasswordDenialReasons***

When a user wants to view a password denial reason, the options are shown in a drop-down list. Multiple reasons are delimited by the pipe (|) character, such as reason1|reason2.

Required	Default Value	Valid Values
no	N/A	<ul style="list-style-type: none"> <li>Deny</li> <li>Password request outside permitted window</li> <li>Other</li> </ul>

### ***ViewPasswordAcknowledgeReasons***

When a user wants to view a password acknowledge reason (for retrospective approval), the options are shown in a drop-down list.

Required	Default Value	Valid Values
no	N/A	Acknowledge

### ***viewPasswordDeclineReasons***

When a user wants to view a password decline reason (for retrospective approval), the options are shown in a drop-down list. Multiple reasons are delimited by the pipe ( | ) character, such as reason1|reason2.

Required	Default Value	Valid Values
no	N/A	<ul style="list-style-type: none"> <li>Decline</li> <li>Other</li> </ul>

### ***lunaPassword***

Luna SA set partition password.

Required	Default Value	Valid Values
no	N/A	password

### ***getLogsMaxSize***

Specifies the file size for server logs, Windows proxy logs, or client logs.

Required	Default Value	Valid Values
no	20 MB	Integer

### ***defaultPasswordViewRequestBanner***

The banner description for the Password View Policy.

Required	Default Value	Valid Values
no	none	Alphanumeric, -, . and space character

## **updateAgent**

Use the updateAgent command to activate and manage the Windows Proxy configuration on the appliance. The Windows Proxy is considered an agent by PAM.

### **Example**

```
capam_command capam=capam_server adminUserId=super cmdName=updateAgent
Agent.ID=1000 Agent.active=true
```

```
Attribute.descriptor1=windows_proxy
```

## **Parameters**

### **Agent.ID**

The unique ID for the agent to be changed.

Required	Default Value	Valid Values
Yes	N/A	Numeric. Retrieve the Agent ID using the searchAgent command.

**Agent.hostName**

The updated value for the agent host name.

Required	Default Value	Valid Values
No. If this parameter is not included, the value is preserved.	N/A	String

**Agent.deviceName**

The updated value for the agent device name.

Required	Default Value	Valid Values
No. If this parameter is not included, the value is preserved.	N/A	String

**Agent.active**

Activates the Windows Proxy agent. Set this parameter to true to activate the agent or false to deactivate to agent.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	false	true, false

**Agent.port**

The port number the agent listens on for incoming requests.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing port value is preserved.	N/A	Integer

**Agent.updatePortFlag**

This command indicates whether the port value is updated. If this value is set to true, the port parameter is set, the port value gets updated.

Required	Default Value	Valid Values
If you are passing the Agent.port parameter, this parameter is required. If this parameter is not included, the existing port value is preserved.	false	true, false

**Agent.acceptPendingFingerprint**

Accepts or denies the pending fingerprint. The fingerprint identifies the Windows Proxy installed on a Windows device.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	false	true, false

**Agent.preserveHostName**

Preserves the agent host name or lets it get overwritten each time the Windows Proxy Agent registers. To prevent the agent host name from being overwritten, set this parameter to true.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	false	true, false

### **Agent.patchStatus**

Disable or enable agent patch upgrade. If this parameter is set to Disabled, the agent does not apply the patch, even if the appliance finds a newer version.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	Disabled	Disabled, Enabled

### **Attribute.descriptor1**

The updated value for the text description field for the Windows Proxy Agent.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	N/A	String

### **Attribute.descriptor2**

The updated value for the text description field for the Windows Proxy Agent.

Required	Default Value	Valid Values
No. If this parameter is not included, the existing value is preserved.	N/A	String

## **updateAuthorization**

Use the updateAuthorization command to change authorization mapping information.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateAuthorization
  Authorization.ID=10
```

```
RequestServer.ID=17 RequestScript.ID=2 Authorization.checkExecutionID=true
  Authorization.executionUser=auser
```

```
Authorization.checkPath=true TargetAlias.ID=6
```

## **Parameters**

### **Authorization.ID**

The unique ID for the authorization mapping to be changed.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchAuthorization to retrieve the Authorization.ID

### **TargetAlias.ID**

The updated value for the target alias ID.

Required	Default Value	Valid Values
TargetAlias.ID or Authorization.targetGroupId	N/A	Numeric. Use searchTargetAlias to retrieve the TargetAlias.ID

### **Authorization.targetGroupId**

The updated value for the target group ID.

Required	Default Value	Valid Values
TargetAlias.ID or Authorization.targetGroupId	N/A	Numeric

### **RequestServer.ID**

The updated value for the request server ID on which the requesting application resides.

Required	Default Value	Valid Values
RequestServer.ID and RequestScript.ID or Authorization.requestGroupId	N/A	Numeric. Use searchRequestServer to retrieve the RequestServer.ID

### **RequestScript.ID**

The updated value for request script ID.

Required	Default Value	Valid Values
RequestServer.ID and RequestScript.ID or Authorization.requestGroupId	N/A	Numeric. Use searchRequestScript to retrieve the RequestScript.ID

### **Authorization.requestGroupId**

The updated value for request group ID.

Required	Default Value	Valid Values
RequestServer.ID and RequestScript.ID or Authorization.requestGroupId	N/A	Numeric

### **Authorization.checkExecutionID**

Set Authorization.checkExecutionID=true to indicate that the execution user ID be validated.

Required	Default Value	Valid Values
yes	false	true, false

**Authorization.executionUser**

A comma delimited list of execution user IDs. The IDs are only validated if Authorization.checkExecutionID=true.

Required	Default Value	Valid Values
yes	N/A	N/A

**Authorization.checkPath**

Set Authorization.checkPath=true to indicate that the script execution path be validated.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	false	true, false

**Authorization.checkFilePath**

Set Authorization.checkFilePath=true to indicate that the script file path be validated.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	false	true, false

**Authorization.checkScriptHash**

Set Authorization.checkScriptHash=true to indicate script hash integrity verification be performed.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	false	true, false

**updateDBClusterMembers**

Use the updateDBClusterMembers command to update database information about a cluster member.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateDbClusterMember
database.ID=db1 active=false
```

**Parameters****database.ID**

Database ID of the cluster member to update

Required	Default Value	Valid Values
yes	N/A	String

**active**

Set this parameter to true to activate the specified cluster member. Specify false to deactivate the member.

Required	Default Value	Valid Values
yes	N/A	true, false

### **method**

Optional synchronization strategy values: "full" or "dump-restore"

Required	Default Value	Valid Values
no	Use <b>dump-restore</b> for MySQL 5.6 or higher and PostgreSQL 9.4 and higher. Use <b>full</b> for Oracle, DB2, SQL Server, and MySQL versions 5.5 or earlier.	full, dump-restore

## **updateDBPassword**

Use this command to change the administrator password for Data Manipulation Language (DML) or Data Definition Language (DDL) user accounts in all Credential Manager databases except DB2. This command can be executed at a secondary site. A DML user can manipulate data within database tables. A DDL user can define the database schema.

When DML and DDL user accounts share the database username, their passwords are changed in the init properties table of Credential Manager. To change database password in DB2 database, use the setInitProperty command.

### **WARNING**

Changing the password directly in the database prevents Credential Manager from operating. Use this command to change the password because Credential Manager uses proprietary key-hiding technology to store the database password securely.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateDBPassword
dbuserType=dml dbusername=admin dbpassword=test

updateLoginCredentials=true
```

### **Parameters**

#### **dbuserType**

The Credential Manager database user type. Data Manipulation Language (DML) or Data Definition Language (DDL).

Required	Default Value	Valid Values
yes	N/A	dml, ddl

#### **dbusername**

The Credential Manager database administrator username.

Required	Default Value	Valid Values
yes	N/A	String



***dbpassword***

Specifies the new Credential Manager database administrator password.

Required	Default Value	Valid Values
yes	N/A	String. In UNIX, passwords with special characters must be enclosed in single quotes.

***updateLoginCredentials***

Indicates whether to update the database user account. Set this parameter to true to update the database. Otherwise, set it to false.

Required	Default Value	Valid Values
no	true	true, false

**updateFilter**

Use the updateFilter command to update a target group or request group filter.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateFilter
  Filter.ID=6 Filter.objectClassId=c.cw.m.ts

  Filter.attribute=hostName Filter.type=contains Filter.expression=Ottawa
```

**Parameters****Filter.ID**

The ID of the filter. It must be an integer greater than or equal to 1.

Required	Default Value	Valid Values
yes	N/A	Integer

**Filter.objectClassId**

The type of object to filter. Class IDs are specific to group type.

Required	Default Value	Valid Values
yes	N/A	c.cw.m.ts, c.cw.m.tp, c.cw.m.ac, c.cw.m.rs, c.cw.m.sc

**Filter.attribute**

The filter attribute. If static, attribute must be ID. If dynamic, attributes are specific to objectClassId.

Required	Default Value	Valid Values
yes	N/A	String

### **Filter.type**

The filter type. If group is static, only equals is valid.

Required	Default Value	Valid Values
yes	N/A	equals, beginswith, contains, endswith, notcontains

### **Filter.expression**

The filter expression. If the group is static, the expression can only be an integer greater than or equal to 1.

Required	Default Value	Valid Values
yes	N/A	String, Integer

## **updateGroup**

Use the updateGroup command to change a target or request group.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateGroup
  Group.ID=5 Group.name="TokyoTargets"
```

```
Group.description="Targets in Tokyo" Group.type=target
```

## **Parameters**

### **Group.ID**

The ID of the group.

Required	Default Value	Valid Values
Group.name or Group.ID	N/A	Integer

### **Group.name**

The name of the target or request group.

Required	Default Value	Valid Values
Group.name or Group.ID	N/A	String

### **Group.description**

The description of the group.

Required	Default Value	Valid Values
no	N/A	String

### **Group.type**

Set this parameter to **requestor** for request groups. Set it to **target** for target groups.

Required	Default Value	Valid Values
yes	N/A	requestor, target

### **Group.dynamic**

Set this parameter to true for dynamic Request or Target groups. Set it to false for static Request or Target groups.

Required	Default Value	Valid Values
no	true	true, false

### **Group.permissions**

Array list object of filters, or XML encoded ArrayList of filters. If not set, the filters are cleared.

Required	Default Value	Valid Values
no	N/A	XML

## **updatePasswordPolicy**

Use the updatePasswordPolicy command to update a password policy.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updatePasswordPolicy
PasswordPolicy.ID=1
PasswordPolicy.name=passwordPolicyName
Attribute.composedOfUpperCaseCharacters=true
Attribute.firstCharacterUpperCase=true
```

### **Parameters**

#### **PasswordPolicy.ID**

The ID of the password policy.

Required	Default Value	Valid Values
yes	null	Numeric

#### **PasswordPolicy.name**

The name of the password policy.

Required	Default Value	Valid Values
yes	null	String

#### **PasswordPolicy.description**

The description of the password policy.

Required	Default Value	Valid Values
no	Blank	String

#### **Attribute.passwordPrefix**

The prefix for all passwords mandated by your password policy.

Required	Default Value	Valid Values
no	None	Constrained by your other settings.

#### **Attribute.composedOfUpperCaseCharacters**

Set to true if you wish to mandate that your password policy contain upper case characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.composedOfLowerCaseCharacters**

Set to true if you wish to mandate that your password policy contain lower case characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.composedOfNumericCharacters**

Set to true if you wish to mandate that your password policy contain numeric characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.composedOfSpecialCharacters**

Set to true if you wish to mandate that your password policy contain an special characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.specialCharacters**

The list of all special characters mandated by your password policy.

Required	Default Value	Valid Values
no	None	!#\$%()*+,-./:;=?@[\\]^_`{ }~

#### **Attribute.firstCharacterUpperCase**

Set to true if you wish to mandate that your password policy contain upper case characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.firstCharacterLowerCase**

Set to true if you wish to mandate that your password policy contain lower case characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.firstCharacterNumeric**

Set to true if you wish to mandate that your password policy contain numeric characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.firstCharacterSpecial**

Set to true if you wish to mandate that your password policy contain an special characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.firstCharacterSpecials**

The list of all special characters mandated by your password policy.

Required	Default Value	Valid Values
no	None	!#\$%()*+,-./:;=?@[\\]^_`{ }~

#### **Attribute.mustNotContainConsecutiveDuplicateCharacters**

Set to true if you wish to mandate that your password policy not allow any repeating characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.mustNotContainAnyDuplicateCharacters**

Set to true if you wish to mandate that your password policy not allow any duplicate characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.mustNotContainCharacters**

Set to true if you wish to mandate that your password policy not contain certain upper case, lower case, or numeric characters.

Required	Default Value	Valid Values
no	false	true, false

#### **Attribute.composedOfMustNotContainCharacters**

The list of all characters not allowed by your password policy. No overlap allowed with special characters.

Required	Default Value	Valid Values
no	Blank	ABCDEFGHIJKLMNOPQRSTUVWXYZabc defghijklmnopqrstuvwxyz0123456789

#### **Attribute.minLength**

Set the minimum length of characters you wish to mandate by your password policy.

Required	Default Value	Valid Values
no	4	Numeric

#### **Attribute.maxLength**

Set the maximum length of characters you wish to mandate by your password policy.

Required	Default Value	Valid Values
no	16	Numeric

#### **Attribute.minIterationsBeforeReuse**

Set the minimum number of iterations before a password can be reused.

Required	Default Value	Valid Values
no	0	Numeric

#### **Attribute.minDaysBeforeReuse**

Set the minimum number of days before a password can be reused.

Required	Default Value	Valid Values
no	0	Numeric

#### **Attribute.enableMaxPasswordAge**

Set to true if you wish to enable Maximum password age in your password policy.

Required	Default Value	Valid Values
no	false	true, false

### **Attribute.maxPasswordAge**

Set the Maximum password age.

Required	Default Value	Valid Values
yes, if Attribute.enableMaxPasswordAge is set to true	None	Numeric

## **updatePasswordViewPolicy**

Use the updatePasswordViewPolicy command to update a password view policy in Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updatePasswordViewPolicy PasswordViewPolicy.ID=7

PasswordViewPolicy.checkinCheckoutRequired=true
PasswordViewPolicy.checkinCheckoutInterval=240
```

### **Parameters**

#### **PasswordViewPolicy.ID**

The ID of the password view policy.

Required	Default Value	Valid Values
yes	N/A	Use searchPasswordViewPolicy to retrieve the ID

#### **PasswordViewPolicy.name**

The updated name of the password view policy.

Required	Default Value	Valid Values
No. If not specified, the existing name is preserved.	N/A	String

#### **PasswordViewPolicy.description**

An updated description of the password view policy.

Required	Default Value	Valid Values
No. If not specified, the existing description is preserved.	N/A	String

**PasswordViewPolicy.changePasswordOnView**

Set PasswordViewPolicy.changePasswordOnView=true to indicate that Credential Manager should change the password after a password view request.

Required	Default Value	Valid Values
No. If not specified, the existing value is preserved.	false	true, false

**PasswordViewPolicy.changePasswordOnSso**

Set PasswordViewPolicy.changePasswordOnSso=true to indicate that Credential Manager should change the password after a password SSO request (retrieved but not viewed).

Required	Default Value	Valid Values
No. If not specified, the existing value is preserved.	false	true, false

**PasswordViewPolicy.passwordChangeInterval**

If the changePasswordOnView parameter is set to true, this parameter determines the amount of time (in minutes) before the password is changed.

Required	Default Value	Valid Values
yes, if PasswordViewPolicy.changePasswordOnView is true	If not specified, the existing value is preserved.	Numeric value greater than 0

**PasswordViewPolicy.checkinCheckoutRequired**

Set this parameter to true to indicate that an account must be checked out to view the password. When checked out, the account password cannot be changed.

Required	Default Value	Valid Values
If not specified, the existing value is preserved.	false	true, false

**PasswordViewPolicy.checkinCheckoutInterval**

This parameter determines the amount of time (in minutes) an account can be checked out before it is automatically checked back in by the system.

Required	Default Value	Valid Values
yes, if PasswordViewPolicy.checkinCheckoutRequired is true	If not specified, the existing value is preserved.	Numeric value greater than 0.

**PasswordViewPolicy.dualAuthorization**



Set the PasswordViewPolicy.dualAuthorization to true to indicate that another user must approve a request to view a password before proceeding. Note that the XML content returned by PAM shows this parameter with name **dualAuthorizationRequired**.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.dualAuthorizationInterval**

This parameter determines the default amount of time (in minutes) a password view request remains active in the system. This setting is valid provided the requesting user does not specify a start and end time for the password view request.

Required	Default Value	Valid Values
yes, if PasswordViewPolicy.dualAuthorization is true.	If not specified, the existing value is preserved	Numeric value greater than 0

#### **PasswordViewPolicy.retrospectiveApprovalRequired**

Set PasswordViewPolicy.retrospectiveApprovalRequired=true to indicate that a request to view a password must be retrospectively approved by an approver.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.approvers**

The list of users who are authorized to approve or deny password requests for accounts that use this password policy.

Required	Default Value	Valid Values
If PasswordViewPolicy.dualAuthorization is true, specify PasswordViewPolicy.approvers or PasswordViewPolicy.approverIDs	If not specified, the existing values are preserved	List of comma-separated usernames. Example: jbauer,mdessler,dpalmer

#### **PasswordViewPolicy.approverIDs**

The list of user IDs who are authorized to approve or deny password requests for accounts that use this password policy.

Required	Default Value	Valid Values
If PasswordViewPolicy.dualAuthorization is true, specify PasswordViewPolicy.approvers or PasswordViewPolicy.approverIDs	Use searchUser to retrieve a list of user IDs. If not specified, the existing values are preserved.	List of comma-separated user IDs. Example: 11,19,15

#### **PasswordViewPolicy.authenticationRequiredSso**

Set this parameter to true to indicate that the requesting user must provide their own password before using the account for auto-connect.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.authenticationRequired**

Set this parameter to true to indicate that the requesting user must provide their own password before viewing the account password.

Required	Default Value	Valid Values
no	true	true, false

#### **PasswordViewPolicy.enableOneClickApproval**

Set this parameter to true to enable dual authorization one click approval. When enabled, dual authorization emails include links that let the approver permit requests without logging into the system.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.PasswordViewRequestMaxInterval**

The maximum Interval between the start and end date of a dual authorization password view request.

Required	Default Value	Valid Values
no	60	Numeric value greater than 0.

#### **PasswordViewPolicy.PasswordViewRequestMaxDays**

The maximum number of days in the future that a password view request can be requested.

Required	Default Value	Valid Values
no	14	Numeric value greater than 0.

#### **PasswordViewPolicy.passwordViewRequestBanner**

The updated banner description for the Password View Policy.

Required	Default Value	Valid Values
no	none	Alphanumeric, -, . and space character

#### **NOTE**

For more information on the following parameters, see their UI equivalents in the [Create a Basic Password View Policy](#) topic.

#### **PasswordViewPolicy.reasonRequiredView**

If set to true, a dialog appears when a user tries to view an Account password. The user selects a Reason and enters a Description and Reference Code to view the password. Select the View Credential (eye icon) for an Account on the Account List page or on the Account Details page.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.reasonRequiredSso**

If set to true, a dialog appears when a user tries to auto-connect. The user selects a Reason and enters an optional Description and optional Reference Code to auto-connect.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.exclusiveCheckoutRequired**

If set to true, this option specifies that credentials are checked in if all connections are closed.

##### **NOTE**

If you select this option, all view properties and the Check-out/Check-in property are unavailable.

If PasswordViewPolicy.exclusiveCheckoutRequired is selected with service desk integration, the Reason Required for View option is selected but disabled. Even though it is selected, the functionality of view password does not work, as exclusive checkout takes precedence. Viewing of a password is disabled when the account is associated with exclusive checkout on auto connect.

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.changePasswordOnSessionEnd**

If set to true, all passwords that are used to log in to target servers are changed when the user session in Privileged Access Manager ends. The connection can end because the user logs out, a session times out, or connectivity is lost. This option does not apply to "View Password."

Required	Default Value	Valid Values
no	false	true, false

#### **PasswordViewPolicy.changePasswordOnConnectionEnd**

If set to true, the password is automatically changed when the user's SSH or RDP connection to a target server ends. The connection can end because the connection times-out, the user terminates the connection, or the connection is lost. This option does not apply to "View Password."

Required	Default Value	Valid Values
no	false	true, false

#### **updatePasswordViewRequestStatus**

Use the updatePasswordViewRequestStatus command to approve or deny a password view request. This command can be run on a secondary site.

## Example

```
capam_command capam=capamServer adminUserID=admin
cmdName=updatePasswordViewRequestStatusPasswordViewRequest.ID=1
PasswordViewRequest.status=approved
```

## Parameters

### **PasswordViewRequest.ID**

The ID of the password view request. Use listPasswordViewRequestByApprover to obtain the PasswordViewRequest.ID

Required	Default Value	Valid Values
yes	N/A	Integer

### ***PasswordViewRequest.status***

Filter results that contain the value that is specified.

Required	Default Value	Valid Values
no	N/A	<b>Dual authorization:</b> "approved" (or 1), "denied" (or 2) <b>Retrospective approval:</b> "acknowledged" (or 9), "declined" (or 10)

### **PasswordViewRequest.statusCode**

The status of the password view request.

Required	Default Value	Valid Values
PasswordViewRequest.statusCode	N/A	1 (approved), 2 (denied) 9 (acknowledged), 10 (declined)

### **PasswordViewRequest.approvalReason**

The approval reason for the password view request.

Required	Default Value	Valid Values
no	N/A	String

### **PasswordViewRequest.approvalReasonDescription**

The approval reason description for the password view request.

Required	Default Value	Valid Values
no	N/A	String

## updateRequestScript

Use the updateRequestScript command to change request application information.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateRequestScript
RequestServer.ID=17 RequestScript.ID=5
```

```
RequestScript.name=myExample.clas RequestScript.executionPath=/opt/cloakware/
cspmclient/examples
```

```
RequestScript.filePath=/opt/cloakware/cspmclient/bin RequestScript.type=java
```

**Parameters****RequestScript.ID**

The unique ID for the request script to be changed.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchRequestScript to retrieve the RequestScript.ID.

**RequestServer.ID**

The updated value for the RequestServer.ID.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchRequestServer to retrieve the RequestServer.ID

**RequestScript.name**

The updated value for the request script name.

Required	Default Value	Valid Values
yes	N/A	String

**RequestScript.executionPath**

The updated value for the location from which the requesting application will be run.

Required	Default Value	Valid Values
yes	N/A	String

**RequestScript.filePath**

The updated value for the location in which the requesting application resides.

Required	Default Value	Valid Values
yes	N/A	N/A

**RequestScript.type**

The updated value for the programming language in which the requesting application is written.

Required	Default Value	Valid Values
yes	N/A	C, C++, C#, csh, Java, ksh, Perl, ksh, VB, VB.NET, VC++, Other

#### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

#### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

## **updateRequestServer**

Use the updateRequestServer command to change request server information.

### **NOTE**

If you want to update the Windows Proxy configuration, use the updateAgent command.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateRequestServer
RequestServer.ID=17
```

```
RequestServer.hostName=myhostname2.mydomain.com Attribute.descriptor1="Lab"
Attribute.descriptor2="Vienna"
```

## **Parameters**

### **RequestServer.ID**

The unique ID for the request server to be changed.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchRequestServer to retrieve RequestServer.ID.

### **RequestServer.hostName**

The updated value for the request server host name.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **RequestServer.deviceName**

The updated value for the request server device name.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **RequestServer.active**

Set RequestServer.active=true to activate the request server. Set RequestServer.active=false to deactivate to request server.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	false	true, false

### **RequestServer.port**

The port number the request server listens on for incoming requests. This value is optional.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	Integer

### **RequestServer.updatePortFlag**

If this value is set to true, and the RequestServer.port value is set, the port flag updates.

Required	Default Value	Valid Values
no. If this parameter is not included, the port is preserved.	false	true, false

### **RequestServer.acceptPendingFingerprint**

This command determines whether to accept or deny the pending fingerprint.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	false	true, false

### **RequestServer.preserveHostName**

Set `RequestServer.preserveHostName=true` to indicate that the request server host name should not be overwritten each time the client registers.

Required	Default Value	Valid Values
no	false	true, false

### **RequestServer.patchStatus**

Disables or enables request server patch upgrade. If this parameter is set to Disabled, the request server does not apply patch, even if newer version found and activated.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	Disabled	Disabled, Enabled

### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

## **updateRequestServerDefaults**

Use the `updateRequestServerDefaults` command to update a request server defaults in Credential Manager.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateRequestServerDefaults
RequestServerDefaults.subnet=192.168.0.0/16
```

```
RequestServerDefaults.active=true RequestServerDefaults.type=CLIENT
RequestServerDefaults.descriptor1=awsApiProxy
```

### **Parameters**

#### **RequestServerDefaults.ID**



The id of the record to delete.

Required	Default Value	Valid Values
yes	N/A	Integer

### **RequestServerDefaults.subnet**

The subnet filter to apply defaults to request servers.

Required	Default Value	Valid Values
yes	N/A	String

### **RequestServerDefaults.type**

The type filter to apply defaults to request servers.

Required	Default Value	Valid Values
yes	N/A	CLIENT, AGENT, ALL

### **RequestServerDefaults.active**

The default setting for RequestServer.active during auto-register.

Required	Default Value	Valid Values
yes	N/A	true, false

### **RequestServerDefaults.descriptor1**

The default setting for Attribute.descriptor1 during auto-register.

Required	Default Value	Valid Values
no	N/A	String

### **RequestServerDefaults.descriptor2**

The default setting for Attribute.descriptor2 during auto-register.

Required	Default Value	Valid Values
no	N/A	String

## **updateRequestServerKey**

Use the updateRequestServerKey command to change the Request Server (Credential Manager client) encryption key.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateRequestServerKey RequestServer.hostName=myhostname.mydomain.com
```

**Parameters****RequestServer.hostName**

The host name of the request server.

Required	Default Value	Valid Values
One of RequestServer.hostName or RequestServer.ID is required.	N/A	String

**RequestServer.ID**

The ID of the request server.

Required	Default Value	Valid Values
One of RequestServer.hostName or RequestServer.ID is required.	N/A	Numeric. Use searchRequestServer to retrieve the RequestServer.ID

**updateRole**

Use the command to change role information in Credential Manager.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateRole Role.ID=11
  Role.name="Patch Management"
```

```
Role.description="Manages Patches" Role.permissions="activatePatch,
  addPatch, deletePatch, getPatchDetail, listPatch, listPatchDetailSummary, updatePatch"
```

**Parameters****Role.ID**

The ID of the role.

Required	Default Value	Valid Values
yes	N/A	Numeric

**Role.name**

The name of the role.

Required	Default Value	Valid Values
yes	N/A	String. A Unique Name in Credential Manager

**Role.description**

The description of the role.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	N/A	String

### **Role.permissions**

A comma delimited list of permissions.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	N/A	String. To see the available list of user permissions, see <a href="#">Add or Modify Credential Manager Roles</a> .

## **updateServerKey**

The updateServerKey command changes the Credential Manager server encryption key. The updateServerKey command reads every encrypted record in the database. The command decrypts the record with the old key, re-encrypts it with the new key, and writes the record back to the database. This command does not take parameters.

### **WARNING**

Before using this command, contact Broadcom Support.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateServerKey
```

## **updateSSHKeyPairPolicy**

Use the updateSSHKeyPairPolicy command to update an existing SSH Key Pair Policy.

### **Example**

```
capam_command capam=capamServer adminUserID=super adminPassword=test
cmdName=updateSSHKeyPairPolicy
SSHKeyPairPolicy.name=Testing SSHKeyPairPolicy.keyType=DSA
SSHKeyPairPolicy.keyLength=512
```

### **Parameters**

#### **SSHKeyPairPolicy.ID**

The policy ID.

Required	Default Value	Valid Values
Yes, if SSHKeyPairPolicy.name is not specified; otherwise no	N/A	An integer greater than or equal to 0

#### **SSHKeyPairPolicy.name**

The policy name.

Required	Default Value	Valid Values
Yes, if SSHKeyPairPolicy.ID is not specified; otherwise no	N/A	String

### **SSHKeyPairPolicy.description**

The policy description.

Required	Default Value	Valid Values
No	N/A	A String

### **SSHKeyPairPolicy.keyType**

The key type.

Required	Default Value	Valid Values
No	N/A	ECDSA or RSA or DSA

### **SSHKeyPairPolicy.keyLength**

The key length.

Required	Default Value	Valid Values
No	N/A	Varies depending on key type. The supported DSA key lengths are 512 bits and 1024 bits. The supported ECDSA key lengths are 256 bits, 384 bits, and 521 bits. The supported RSA key lengths are 1024 bits, 2048 bits, and 4096 bits..

## **updateTargetAccount**

Use the updateTargetAccount command to change target account information, including the target account password. Alternatively, use updateTargetAccountPassword to change the password. More parameters may be required, depending on the Target Application Type. For a description of these additional parameters, look up the appropriate turnkey target connector.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetAccountvTargetAccount.ID=12
```

```
TargetServer.hostName=myhostname.mydomain.com
TargetApplication.name=myApplication TargetAccount.userName=sysop1
```

```
TargetAccount.password='sys0p!@2' TargetAccount.cacheBehavior=useServerFirst
TargetAccount.cacheDuration=17
```

**Parameters****TargetAccount.ID**

The unique ID for the target account to be changed.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchTargetAccount to retrieve the TargetAccount.ID

**TargetApplication.ID**

The updated value for TargetApplication.ID.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchTargetApplication to retrieve the TargetApplication.ID

**TargetAccount.userName**

The updated value for the target account user name.

Required	Default Value	Valid Values
yes.	N/A	String

**TargetAccount.password**

The updated value for the target account password.

Required	Default Value	Valid Values
no. If this parameter is not included, the password is unchanged	N/A	If a password policy is assigned to the target application, this value must adhere to the password policy. In addition to password policy requirements, a password must be minimum of 1 character and a maximum of 255 characters in length.

**TargetAccount.cacheAllow (Deprecated)**

Deprecated Parameter, use TargetAccount.cacheBehavior: Set TargetAccount.cacheAllow=true to have credentials for this account that is cached in the Credential Manager client.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	true, false

**TargetAccount.cacheBehavior**

To use the credentials that are cached at the target account first, set TargetAccount.cacheBehavior=useCacheFirst.  
To use the credentials that are cached at this target account but contact the Server first, set

TargetAccount.cacheBehavior=useServerFirst. To ensure that the credentials for this account are not cached at the target account, set TargetAccount.cacheBehavior=noCache.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	useCacheFirst	useCacheFirst, useServerFirst, noCache

### **TargetAccount.cacheDuration**

Use TargetAccount.cacheDuration to specify the number of days the account credentials are permitted to reside in a Credential Manager client cache.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	1-356

### **TargetAccount.privileged**

Set TargetAccount.privileged=true to indicate that this account is a privileged account. Set TargetAccount.privileged=false to indicate that this account is an application-to-application account.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	true, false

### **TargetAccount.accessType**

Use this text field for reference purposes.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	N/A	String

### **TargetAccount.synchronize**

Set TargetAccount.synchronize=true to indicate that the password that is stored in the Credential Manager database should be synchronized with the password on the target system. This functionality is not supported with Target Application Type Generic.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	true, false

### **Attribute.changePasswordAfterViewing (Deprecated)**

This parameter is no longer used.: Set Attribute.changePasswordAfterViewing=true to indicate that Credential Manager should change the password after a password view request (either from the GUI or CLI). This feature applies only to

accounts where TargetAccount.synchronize=true. This parameter is ignored if the Change Password After Viewing feature has been disabled on the Credential Manager server.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	true, false

#### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

#### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

#### **PasswordViewPolicy.ID**

The ID of a PasswordViewPolicy attached to this account.

Required	Default Value	Valid Values
No. If this parameter is not included, the value is preserved.	N/A	Numeric

#### **TargetAlias.name**

A comma-separated list of TargetAlias.name values. This parameter depends on the value of useTargetAliasNameParameter being true.

Required	Default Value	Valid Values
no. If not specified and useTargetAliasNameParameter is set to true, all associated target aliases are deleted	N/A	Comma-separated string

#### **useTargetAliasNameParameter**

If this parameter is set to true, Credential Manager adds target aliases for this account. If the value is false, the aliases are not used.

Required	Default Value	Valid Values
no.	false	true, false

#### **TargetAccount.compoundAccount**

If this parameter is set to true, Credential Manager adds compound target servers for this account, using the values of the `TargetAccount.compoundServerIDs` parameter. If the value is false, the compound target servers are not used.

Required	Default Value	Valid Values
no.	false	true, false

### **TargetAccount.compoundServerIDs**

This parameter adds (true) or deletes (false) compound servers to the list of compound server IDs for the target account.

Required	Default Value	Valid Values
no.	false	true, false

### **passwordIsBase64Encoded**

If this parameter is set to true, the specified password is Base64-encoded. The parameters instruct Credential Manager to decode the password before storing it.

Required	Default Value	Valid Values
no.	false	true, false

## **updateTargetAccountDescriptor**

Use the `updateTargetAccountDescriptor` command to change the descriptor value of a target account.

### **Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetAccountDescriptor
```

```
TargetAccount.ID=5 Attribute.descriptor1=testvalue1
Attribute.descriptor2=testvalue2
```

## **Parameters**

### **TargetServer.hostName**

The host name for the target server on which the target account resides.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This value must match a target server name registered in Credential Manager.

### **TargetApplication.name**



The target application name on which the target account is hosted.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This value must match a target application name registered in Credential Manager.

### **TargetAccount.userName**

The user name for the target account.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This target account name must be unique for a given target application. This name must match the user name in the target application.

### **TargetAccount.ID**

The unique identifier of the target account. This value is required if TargetServer.hostName, TargetApplication.name and TargetAccount.userName are not specified.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	Numeric. Use searchTargetAccount to retrieve the TargetAccount.ID

### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic target groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic target groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

## **updateTargetAccountPassword**

Use the updateTargetAccountPassword command to change a target account password. The password can be specified or automatically generated based on the associated password policy. By default, this command works only for synchronized accounts. Set the **allowUnsynchronized** parameter to true to change the default nature.

**Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetAccountPassword
TargetServer.hostName=myhostname.mydomain.com

TargetApplication.name=myApplication TargetAccount.userName=sysopl
```

**Parameters****TargetServer.hostName**

The host name for the target server on which the target account resides.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This value must match a target server name registered in Credential Manager.

**TargetApplication.name**

The target application name on which the target account is hosted.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This value must match a target application name registered in Credential Manager.

**TargetAccount.userName**

The user name for the target account.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	String. This target account name must be unique for a given target application. This name must match the user name in the target application.

**TargetAccount.ID**

The unique identifier of the target account. This value is required if TargetServer.hostName, TargetApplication.name and TargetAccount.userName are not specified.

Required	Default Value	Valid Values
TargetServer.hostName, TargetApplication.name, and TargetAccount.userName; or TargetAccount.ID	N/A	Numeric. Use searchTargetAccount to retrieve the TargetAccount.ID.

**groupId**

The unique identifier of the target group for which the passwords will be updated.

Required	Default Value	Valid Values
no	N/A	Numeric. Use searchGroup to retrieve the groupId.

**password**

The password for the target account.

Required	Default Value	Valid Values
no	generated password	The password must conform to any applied password policies.

**confirmPassword**

The password for the target account.

Required	Default Value	Valid Values
no	generated password	The password must conform to any applied password policies. This must match the password value.

**allowUnsynchronized**

Allows the password to be updated for non-synchronized accounts.

Required	Default Value	Valid Values
no	false	String. Set the value to true to allow updates of unsynchronized accounts.

**TargetAccount.passwordVerified**

boolean

Required	Default Value	Valid Values
No	nothing (update all accounts)	true to update only verified accounts, false to verify accounts that failed verification

**updateTargetAlias**

Use the updateTargetAlias command to change target alias information.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateTargetAlias
  TargetAlias.ID=12 TargetAccount.ID=5

TargetAlias.name=myaliasname
```

**Parameters****TargetAlias.ID**

The unique ID for the target alias to be changed.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchTargetAlias to retrieve the TargetAlias.ID

**TargetAccount.ID**

The updated value for the TargetAccount.ID.

Required	Default Value	Valid Values
yes	N/A	Numeric. Use searchTargetAccount to retrieve the TargetAccount.ID

**TargetAlias.name**

The updated value for the target alias name

Required	Default Value	Valid Values
no. If this parameter is not included, the value is set to null	N/A	String. The target alias name must be unique within the Credential Manager server.

**updateTargetApplication**

Use the updateTargetApplication command to change target application information. Additional parameters might be required, depending on the Target Application Type. For a description of these other parameters, look up the appropriate turnkey target connector. Prior to running updateTargetApplication, use searchTargetApplication to retrieve current parameter values.

**Example**

```
capam_command capam=capamServer adminUserID=admin
cmdName=updateTargetApplication TargetApplication.ID=5

TargetServer.ID=8 TargetApplication.name=myApplication
TargetApplication.type=Generic
```

**Parameters****TargetApplication.ID**

The unique ID for the target application to be changed.

Required	Default Value	Valid Values
yes	N/A	Use SearchTargetApplication to retrieve the TargetApplication.ID

### **TargetServer.ID**

The updated value for the ID of the target server on which the target application is hosted.

Required	Default Value	Valid Values
yes	N/A	Use searchTargetServer to retrieve the TargetServer.ID

### **TargetApplication.name**

The updated value for the name of the target application.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **TargetApplication.type**

The updated value for the target application connector name. Valid values depend upon which target connectors are installed on your system. If this parameter is not included, the target application type is preserved.

Required	Default Value	Valid Values
yes	N/A	See the addTargetApplication command for a list of valid application types.

### **PasswordPolicy.name**

The updated value for the name of the password policy that is applied to all accounts on associated with this application.

Required	Default Value	Valid Values
no. If PasswordPolicy.name or PasswordPolicy.ID is not included, the password policy is preserved.	N/A	If a password policy is not specified, manually entered passwords are not validated against a policy. In addition, Credential Manager generated passwords use the Credential Manager default password policy.

### **PasswordPolicy.ID**

The updated value for the ID of the password policy that is applied to all accounts on associated with this application.

Required	Default Value	Valid Values
no. If PasswordPolicy.name or PasswordPolicy.ID is not included, the password policy is preserved.	N/A	Use searchPasswordPolicy to retrieve this ID. If a password policy is not selected, manually entered passwords are not validated against a policy. In addition, Credential Manager-generated passwords use the default password policy.

#### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

#### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

#### **Attribute.enableAutoConnectTargetAccount**

A boolean value to enable / disable autoConnectTargetAccount for an application instance.

Required	Default Value	Valid Values
no	false	true, false

## **updateTargetServer**

Use the updateTargetServer command to change target server information.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateTargetServer
TargetServer.ID=17 TargetServer.hostName=myhostname2.mydomain.com
Attribute.descriptor1="Lab" Attribute.descriptor2="Vienna"
```

## **Parameters**

### **TargetServer.ID**

The unique ID for the target server to be changed.

Required	Default Value	Valid Values
yes. Required only if the TargetServer.hostName is changed.	N/A	Use searchTargetServer to retrieve the TargetServer.ID.

### **TargetServer.hostName**

The updated value for the host name of target server.

Required	Default Value	Valid Values
yes	N/A	This must be the fully qualified host name as entered in the DNS server.

### **TargetServer.deviceName**

The updated value for the device name of target server.

Required	Default Value	Valid Values
no	N/A	String

### **Attribute.descriptor1**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

### **Attribute.descriptor2**

The updated value for the text description field. Use this field as a filter for dynamic authorization groupings.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String

## **updateUser**

Use the updateUser command to change Credential Manager user information.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateUser
User.userID=demo User.password=demo123$
User.authenticationType=CSPM User.status=ACTIVE User.userGroupIDS=1,2
User.firstName=Demo User.lastName=User
```

### **NOTE**

Reactivating a suspended user clears the user's deactivation reason in the UI. Suspending an active user automatically sets the user's deactivation reason to **Other** in the UI.

**Parameters****User.userID**

The unique user name for the Credential Manager user to be changed.

Required	Default Value	Valid Values
yes	N/A	String

**User.password**

The updated value for the user's password.

Required	Default Value	Valid Values
This parameter is required if the authentication type is Credential Manager.	N/A	String. Credential Manager passwords must contain 6-16 characters containing at least one alphabetic, one numeric, and one special character.

**User.authenticationType**

The updated value for authentication type of the user.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	CSPM	CSPM, LDAP, SecurID, Kerberos, X509 or any installed authentication connector. For a complete list of installed authentication connectors, see \$CSPM_SERVER_HOME/cspmserver/config/authentication.xml f

**User.status**

The updated value for the user account status.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	ACTIVE	ACTIVE or SUSPENDED. Set to ACTIVE for active user accounts and to SUSPENDED to suspend a user account.

**User.userGroupIDS**

The updated value for IDs of the User Groups to assign to this user.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	Numeric IDs delimited by comma. Use listUserGroups to retrieve User Group IDs. Alternatively, you can specify the User.userGroupNames parameter. Values must match User Groups registered in Credential Manager.

**User.userGroupNames**



The updated value for names of the User Groups to assign to this user.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is preserved.	N/A	String containing the User Group names delimited by comma. Values must match User Groups registered in Credential Manager.

### **User.firstName**

The updated value for the first name of the user.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	N/A	String

### **User.lastName**

The updated value for the last name of the user.

Required	Default Value	Valid Values
no. If this parameter is not included, the value is reset to null.	N/A	String

### **User.email**

The updated value for the email address of the user.

Required	Default Value	Valid Values
no	N/A	String

### **User.viewType**

Determines what UI view this user has access to, administrative or general

Required	Default Value	Valid Values
no. If this parameter is not included, the existing value is preserved	N/A	admin, general

## **updateUserGroup**

Use the updateUserGroup command to change information for a user group.

### **Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=updateUserGroup
  UserGroup.ID=2 UserGroup.name=updatedUserGroupName
  UserGroup.description="Updated user group description" UserGroup.roleID=11
  UserGroup.groups=3,4
```

**Parameters****UserGroup.ID**

The user group ID.

Required	Default Value	Valid Values
yes	N/A	Numeric. A unique user group ID

**UserGroup.name**

The user group name.

Required	Default Value	Valid Values
yes	N/A	String. A unique user group name

**UserGroup.description**

The description of the group.

Required	Default Value	Valid Values
no. If this parameter is not included it will be reset to null.	N/A	String

**UserGroup.roleID**

The role identifier of this group.

Required	Default Value	Valid Values
yes	N/A	Numeric. This value must match a role ID registered in Credential Manager.

**UserGroup.groups**

A comma delimited list of group IDs.

Required	Default Value	Valid Values
no. If this parameter is not included it will be reset to null.	N/A	Numeric. Comma delimited list of group IDs

**NOTE**

Each dynamic target group referenced in the listed group IDs *must have at least one* filter defined. If not, the group is not updated.

**UserGroup.readOnly**

The read only flag for the user group.

Required	Default Value	Valid Value
no	N/A	true. False is not a valid value.

## updateUserPassword

Use the updateUserPassword command to change a user account password. If the account authentication type is CSPMA or Credential Manager, a user can only update their own password.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=updateUserPassword
User.password=tlger@
```

### Parameters

#### User.password

The new password.

Required	Default Value	Valid Values
yes	N/A	String. Credential Manager user passwords must be between 6 and 16 characters in length, and can contain alphabetical, numeric and special characters.

## updateUserStatus

Use the updateUserStatus command to change the status of a user account to ACTIVE or SUSPENDED. When the status is set to ACTIVE, the number of failed login attempts is reset to 0.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=updateUserStatus
userID=demo status=ACTIVE
```

### Parameters

#### *User.userID*

The user name.

Required	Default Value	Valid Values
yes	N/A	String

#### *User.status*

The new user status.

Required	Default Value	Valid Values
yes	N/A	ACTIVE, SUSPENDED

## verifyAccountPassword

Use the verifyAccountPassword command to validate the account password of a synchronized user or of all synchronized accounts in a target group. You can indicate whether to validate accounts that passed or failed verification.

### Example

```
capam_command capam=capamServer adminUserID=admin cmdName=verifyAccountPassword
groupID=1234
```

```
TargetAccount.passwordVerified=false
```

### Parameters

#### TargetAccount.ID

The target account ID.

Required	Default Value	Valid Values
Either this or groupID must be specified.	N/A	A whole number

#### groupID

The target group ID

Required	Default Value	Valid Values
Either this or TargetAccount.ID must be specified.	N/A	A whole number

#### TargetAccount.passwordVerified

This parameter determines which accounts get verified.

Required	Default Value	Valid Values
No	nothing (verify all accounts)	true - validates only verified accounts false - validates accounts that failed verification

## verifyDBHash

The verifyDBHash command confirms the hash value of most base model objects that are stored in the Credential Manager database. Use this command to verify the data integrity of the following objects:

All Agents	Authorizations
Request Servers	Scripts
Target Accounts	Target Aliases
Target Applications	Target Servers

This command has no parameters.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=verifyDBHash
```

**viewAccountPassword**

Use the `viewAccountPassword` command to retrieve a target account password.

**Example**

```
capam_command capam=capamServer adminUserID=admin cmdName=viewAccountPassword
  TargetAccount.ID=5

reason="Power outage reason" reasonDetails="Recover Tuesday am"
```

**Parameters****TargetAccount.ID**

The ID of the target account for which you are seeking the password.

Required	Default Value	Valid Values
yes	N/A	Use <code>searchTargetAccount</code> to retrieve the <code>TargetAccount.ID</code> .

**adminUserID**

Your Credential Manager user name.

Required	Default Value	Valid Values
yes	N/A	String. User must be a valid Credential Manager user with permission to view passwords.

**adminPassword**

Your Credential Manager user password.

Required	Default Value	Valid Values
yes	N/A	String

**reason**

The reason that you are requesting a password view.

Required	Default Value	Valid Values
Conditionally required when "Reason Required for View" or Reason Required for Auto-Connect" is enabled in the Password View Policy.	N/A	String

### reasonDetails

Detailed description of why you want to view the password.

Required	Default Value	Valid Values
Conditionally required when "Reason Required for View" or Reason Required for Auto-Connect" is enabled in the Password View Policy.	N/A	String

### selectedComponent

Compound server ID.

Required	Default Value	Valid Values
no	N/A	Integer

### ssoType

SSO type implies that a password was used but not viewed, so change is controlled by `CPoV && AllowCpovOnSso`.

Required	Default Value	Valid Values
no	N/A	"Browser", "RDP", "SSH", "VNC", "AWSAPI", "Telnet", "Other"

### PasswordViewRequest.requestPeriodStart

If the account password view policy has enabled dual authorization, this parameter specifies the start time of the password view request.

Required	Default Value	Valid Values
no	N/A	Date string, of the format <code>yyyy-MM-dd hh:mm:ss</code>

### PasswordViewRequest.requestPeriodEnd

If the account password view policy has enabled dual authorization, this parameter specifies the end time of the password view request.

Required	Default Value	Valid Values
no	N/A	Date string, of the format <code>yyyy-MM-dd hh:mm:ss</code>

### referenceCode

Reference Code.

Required	Default Value	Valid Values
Conditionally required when "Reason for View" or "Reason Required for Auto-Connect" is enabled in the Password View Policy.	N/A	S

### **PasswordViewRequest.comments**

Comments that the user wants to add to the view password request.

Required	Default Value	Valid Values
no	N/A	String

## **Secrets Management CLI Commands**

You can use the Remote CLI to control and configure Secrets Management. This command-line interface allows administrators to provide scripted functionality to complete management and integration tasks. The interface supports a subset of features that are available through the GUI.

Use the table of contents to access the command descriptions.

### **addVault**

Use this command to add a vault to PAM.

#### **Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=addVault "Vault.name=test
vault" "Vault.description=my test vault" Vault.userIDs="1001,2001" Vault.userRoleIDs="5001,6001"
Vault.userGroupIDs="3001,4001" Vault.userGroupRoleIDs="7001,8001"
```

### **Parameters**

#### **Vault.name**

Specifies the name of the vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.description**

Specifies the description of the vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userIDs**

A comma-delimited list of user IDs (users) that are associated with this vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userRoleIDs**

A comma delimited list of role IDs. There must be a one-to-one mapping between the Vault.userIDs and Vault.userRoleIDs. For example, the first user ID in the Vault.userIDs list is assigned the first role ID from Vault.userRoleIDs. The second user ID in the Vault.userIDs list is assigned the second role ID from the Vault.userRoleIDs list, and so on.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userGroupIDs**

A comma-delimited list of user group IDs that are associated with this vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userGroupRoleIDs**

A comma delimited list of role IDs. There must be a one-to-one mapping between the Vault.userGroupIDs and Vault.userGroupRoleIDs. For example, the first user ID in the Vault.userGroupIDs list is assigned the first role ID from Vault.userGroupRoleIDs. The second user ID in the Vault.userGroupIDs list is assigned the second role ID from the Vault.userGroupRoleIDs list, and so on.

Required	Default Value	Valid Values
yes	N/A	String

## **updateVault**

Use this command to update a vault in PAM.

### **Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=updateVault Vault.ID=1001
"Vault.name=test vault" Vault.userIDs="1001,2001" Vault.userRoleIDs="5001,6001"
Vault.userGroupIDs="3001,4001" Vault.userGroupRoleIDs="7001,8001"
```

## **Parameters**

### **Vault.ID**

Specifies the identifier of the vault.

Required	Default Value	Valid Values
yes	N/A	Numeric

### **Vault.name**



Specifies the name of the vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.description**

Specifies the description of the vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userIDs**

A comma-delimited list of user IDs (users) that are associated with this vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userRoleIDs**

A comma delimited list of role IDs. There must be a one-to-one mapping between the Vault.userIDs and Vault.userRoleIDs. For example, the first user ID in the Vault.userIDs list is assigned the first role ID from Vault.userRoleIDs. The second user ID in the Vault.userIDs list is assigned the second role ID from the Vault.userRoleIDs list, and so on.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userGroupIDs**

A comma-delimited list of user group IDs that are associated with this vault.

Required	Default Value	Valid Values
yes	N/A	String

#### **Vault.userGroupRoleIDs**

A comma delimited list of role IDs. There must be a one-to-one mapping between the Vault.userGroupIDs and Vault.userGroupRoleIDs. For example, the first user ID in the Vault.userGroupIDs list is assigned the first role ID from Vault.userGroupRoleIDs. The second user ID in the Vault.userGroupIDs list is assigned the second role ID from the Vault.userGroupRoleIDs list, and so on.

Required	Default Value	Valid Values
yes	N/A	String

## getVault

Use this command to return information about a vault.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=getVault Vault.name="test vault"
Vault.ID=1001
```

### Parameters

#### Vault.ID

Specifies the identifier of the vault. This value is required if Vault.name is not set.

Required	Default Value	Valid Values
yes (If Vault.name is not set)	N/A	Numeric

#### Vault.name

Specifies the name of the vault.

Required	Default Value	Valid Values
yes	N/A	String

## deleteVault

Use this command to delete an existing vault.

You can only delete an empty vault. You must delete all secrets from a vault before you can delete it. You cannot restore a deleted Vault. However, deleting the vault does not delete the users or user groups that are assigned to them.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=deleteVault Vault.ID=18
```

### Parameters

#### Vault.name

Specifies the identifier of the vault.

Required	Default Value	Valid Values
yes	N/A	Numeric

## viewSecretPassword

Use the viewSecretPassword command to return a secret password value in clear text.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=viewSecretPassword
Secret.vaultName="test vault" Secret.ID=10001
```

**Parameters****Secret.ID**

Specifies the identifier of the secret.

Required	Default Value	Valid Values
yes	N/A	String

**Secret.vaultName**

Specifies the name of the vault to which this secret belongs.

Required	Default Value	Valid Values
yes	N/A	String. The unique name of the device name in PAM.

**listVaults**

Use this command to retrieve a list of vaults in PAM.

**Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=listVaults
```

**Parameters****Vault.columnNames**

Use `Vault.columnNames` to specify the filter criteria when searching for vaults.

Required	Default Value	Valid Values
no	name	String; name, description

**Vault.columnValues**

Use `Vault.columnValues` to specify the filter criteria when searching for vaults.

Required	Default Value	Valid Values
no	N/A	String

**Page.Number**

Specifies which page to return when the results are divided among multiple pages. This parameter works in conjunction with `Page.Size`.

Required	Default Value	Valid Values
no	1	Numeric

**Page.Size**

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	30	Numeric

### **Sort.Property**

Use `Sort.Property` to specified which field to use when sorting the result.

Required	Default Value	Valid Values
no	name	String; name description

### **Sort.Direction**

Specifies the alphabetical order of the results returned. Set `Sort.Direction=true` to have the results presented in descending order. Set `Sort.Direction=false` to have the results presented in ascending order.

Required	Default Value	Valid Values
no	false	String; true, false

## **addSecret**

Use this command to add a secret to a specified vault. The `addSecret` command allows up to 12 parameters. The `secret.name`, `secret.typeID`, and `secret.value`, `secret.formatID` parameters are required.

### **Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=addSecret Secret.name="mySecret"
Secret.aliases="mySecret" Secret.typeID=1 Secret.vaultID=24001 "Secret.value=keep me secret"
```

## **Parameters**

### **Secret.name**

Specifies the name of the secret.

Required	Default Value	Valid Values
yes	N/A	String

### **Secret.aliases**

Specifies the alias of the secret.

Required	Default Value	Valid Values
yes	N/A	String. Separate multiple values by commas.

### **Secret.descriptor1**

Specifies the first descriptor of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.descriptor2**

Specifies the second descriptor of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.typeID**

Specifies the identifier of the secret type associated with the secret.

Required	Default Value	Valid Values
yes	N/A	Numeric

### **Secret.vaultID**

Specifies the identifier of the vault to which the secrets should be added.

Required	Default Value	Valid Values
no	N/A	Numeric

### **Secret.value**

Specifies the value of the secret.

Required	Default Value	Valid Values
yes	N/A	String

### **Secret.formatID**

Specifies the identifier of the secret format associated with the secret.

Required	Default Value	Valid Values
yes	N/A	String

### **Secret.autoExpire**

Specifies whether the secret expires at a specified date. Set this value to `true` to cause the secret to expire. Expired secrets are not removed from the system, but cannot be used. Use this parameter in conjunction with the `secret.autoExpireDate` parameter.

Required	Default Value	Valid Values
no	N/A	String; <code>true</code> , <code>false</code>

### **Secret.autoExpireDate**

Specifies the date and time that the secret should expire. Use this parameter in conjunction with the `secret.autoExpire` parameter.

Required	Default Value	Valid Values
no	N/A	Format: MM/dd/yyyy HH:mm:ss

### **Secret.autoDelete**

Specifies whether the secret is deleted at a specified date. Set this value to `true` to cause the secret to be deleted at the top of the hour. Deleted secrets are removed from the system. Use this parameter in conjunction with the `secret.autoDeleteDate` parameter.

Required	Default Value	Valid Values
no	N/A	String; <code>true</code> , <code>false</code>

### **Secret.autoDeleteDate**

Specifies the date and time that the secret should expire. Secrets are deleted at the top of the hour specified here. Use this parameter in conjunction with the `secret.autoDelete` parameter.

Required	Default Value	Valid Values
no	N/A	Format: MM/dd/yyyy HH:mm:ss

## **updateSecret**

Use this command to update a secret in a specified vault. The `updateSecret` command allows up to 13 parameters. The `secret.ID` parameter is required.

### **Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=updateSecret Secret.ID=35001
Secret.name="mySecret" Secret.vaultID=24001 "Secret.value=updated secret"
```

## **Parameters**

### **Secret.ID**

Specifies the identifier of the secret.

Required	Default Value	Valid Values
yes	N/A	Numeric

### **Secret.name**

Specifies the name of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.aliases**

Specifies the alias of the secret.

Required	Default Value	Valid Values
no	N/A	String. Separate multiple values by commas.

### **Secret.descriptor1**

Specifies the first descriptor of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.descriptor2**

Specifies the second descriptor of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.typeID**

Specifies the identifier of the secret type associated with the secret.

Required	Default Value	Valid Values
no	N/A	Numeric

### **Secret.vaultID**

Specifies the identifier of the vault to which the secrets should be added.

Required	Default Value	Valid Values
no	N/A	Numeric

### **Secret.value**

Specifies the value of the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.formatID**

Specifies the identifier of the secret format associated with the secret.

Required	Default Value	Valid Values
no	N/A	String

### **Secret.autoExpire**

Specifies whether the secret expires at a specified date. Set this value to `true` to cause the secret to expire. Expired secrets are not removed from the system, but cannot be used. Use this parameter in conjunction with the `secret.autoExpireDate` parameter.

Required	Default Value	Valid Values
no	N/A	String; <code>true</code> , <code>false</code>

### **Secret.autoExpireDate**

Specifies the date and time that the secret should expire. Use this parameter in conjunction with the `secret.autoExpire` parameter.

Required	Default Value	Valid Values
no	N/A	Format: MM/dd/yyyy HH:mm:ss

### **Secret.autoDelete**

Specifies whether the secret is deleted at a specified date. Set this value to `true` to cause the secret to be deleted at the top of the hour. Deleted secrets are removed from the system. Use this parameter in conjunction with the `secret.autoDeleteDate` parameter.

Required	Default Value	Valid Values
no	N/A	String; <code>true</code> , <code>false</code>

### **Secret.autoDeleteDate**

Specifies the date and time that the secret should expire. Secrets are deleted at the top of the hour specified here. Use this parameter in conjunction with the `secret.autoDelete` parameter.

Required	Default Value	Valid Values
no	N/A	Format: MM/dd/yyyy HH:mm:ss

## **getSecret**

Use this command to return information about a secret.

### **Example**

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=getSecret Secret.ID=1001
```

## **Parameters**

### **Secret.ID**

Specifies the identifier of the secret.

Required	Default Value	Valid Values
yes	N/A	String



## listSecrets

Use this command to retrieve a list of secrets in PAM.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=listSecrets
```

### Parameters

#### Secret.columnNames

Use `Secret.columnNames` to specify the filter criteria when searching for secrets.

Required	Default Value	Valid Values
no	name	String; name, description

#### Secret.columnValues

Use `Secret.columnValues` to specify the filter criteria when searching for secrets.

Required	Default Value	Valid Values
no	N/A	String

#### Page.Number

Specifies which page to return when the results are divided among multiple pages. This parameter works in conjunction with `Page.Size`.

Required	Default Value	Valid Values
no	1	Numeric

#### Page.Size

Specifies the number of records to return on each page.

Required	Default Value	Valid Values
no	30	Numeric

#### Sort.Property

Use `Sort.Property` to specified which field to use when sorting the result.

Required	Default Value	Valid Values
no	name	String; name description

#### Sort.Direction

Specifies the alphabetical order of the results returned. Set `Sort.Direction=true` to have the results presented in descending order. Set `Sort.Direction=false` to have the results presented in ascending order.

Required	Default Value	Valid Values
no	false	String; true, false

## deleteSecret

Use this command to delete a secret or list of secrets. Deleting a secret removes it permanently from the vault and from PAM. You can neither restore nor recover a deleted secret. Secrets are deleted at the top of the hour.

### Example

```
cspmserver_admin cspmHostName=paServer adminUserID=admin cmdName=deleteSecret
Secret.IDs="1001,2001"
```

### Parameters

#### Secret.ID

Specifies the identifier of the secret.

Required	Default Value	Valid Values
yes	N/A	String; separate multiple values with commas.

## Integrate Applications with the Credential Manager A2A Client

This content describes the methods that Credential Manager provides for integration.

### A2A client on all platforms

Language	Integration Method	Example
Java	CSPMClient.jar See <a href="#">Integrate Applications Using Java</a> .	<a href="#">Integrate Java Applications with the Credential Manager A2A Client</a> .

### A2A client on UNIX

Language	Integration Method	Example
Perl	cspmclient See <a href="#">Integrate Applications Using the A2A Client</a> .	<a href="#">Integrate a Perl Script with A2A Client on UNIX or AIX</a> .
C++		<a href="#">Integrate a C or C++ Application with A2A Client on UNIX or AIX</a> .
C		<a href="#">Integrate a C or C++ Application with A2A Client on UNIX or AIX</a> .
Korn Shell		<a href="#">Integrate a Korn Shell Script with A2A Client on UNIX or AIX</a> .
C Shell		<a href="#">Integrate a C Shell Script with A2A Client on UNIX or AIX</a> .
PHP		<a href="#">Integrate a PHP Script with A2A Client on UNIX</a> .
Python		<a href="#">Integrate a Python Script with A2A Client on UNIX and AIX</a> .

**A2A client on Windows**

Language	Integration Method	Example
Perl	cspmclient.exe See <a href="#">Integrate Applications Using the A2A Client</a> .	<a href="#">Integrate a Perl Script with A2A Client on Windows.</a>
PowerShell	cspmclient.exe See <a href="#">Integrate Applications Using the A2A Client</a> .	<a href="#">Integrate a PowerShell Script with A2A Client on Windows.</a>
Visual Basic Visual C++ C#	cspmclientc.dll See <a href="#">Integrate Windows Applications and Scripts Using a Windows DLL</a> .	<a href="#">Integrate a Visual Basic Application.</a> <a href="#">Integrate a Visual C++ Application.</a> <a href="#">Integrate a C#.NET Application using IIS Application Server.</a>
Visual Basic Script	cspmclientatl.dll See <a href="#">Integrate Windows Applications and Scripts Using a Windows DLL</a> .	<a href="#">Integrate a Visual Basic, Java, or Windows Script.</a>
JavaScript	cspmclientatl.dll See <a href="#">Integrate Windows Applications and Scripts Using a Windows DLL</a> .	<a href="#">Integrate a Visual Basic, Java, or Windows Script.</a>

**A2A 64-bit Client on all platforms**

Language	Integration Method	Example
Java	CSPMClient.jar See <a href="#">#unique_1900</a> .	<a href="#">Integrate Java Applications with the Credential Manager A2A Client.</a>

**A2A 64-bit Client on UNIX and AIX**

Language	Integration Method	Example
Perl	cspmclient64 See <a href="#">#unique_1902</a> .	<a href="#">Integrate a Perl Script with A2A Client on UNIX or AIX</a>
C++		<a href="#">Integrate a C or C++ Application with A2A Client on UNIX or AIX</a>
C		<a href="#">Integrate a C or C++ Application with A2A Client on UNIX or AIX</a>
Korn Shell		<a href="#">Integrate a Korn Shell Script with A2A Client on UNIX or AIX</a>
C Shell		.
PHP <b>Note: PHP is not supported on AIX.</b>		<a href="#">Integrate a PHP Script with A2A Client on UNIX</a>
Python		<a href="#">Integrate a Python Script with A2A Client on UNIX and AIX</a>

**A2A 64-bit Client on Windows**

Language	Integration Method	Example
Perl	cspmclient64.exe See <a href="#">Integrate Applications Using the A2A Client</a> .	<a href="#">Integrate a Perl Script with A2A Client on Windows.</a>
PowerShell	cspmclient64.exe See <a href="#">Integrate Applications Using the A2A Client</a> .	<a href="#">Integrate a PowerShell Script with A2A Client on Windows.</a>

Visual Basic Visual C++ C#	cspmclientc64.dll See <a href="#">Integrate Windows Applications and Scripts Using a Windows DLL</a> .	<a href="#">Integrate a Visual Basic Application.</a> <a href="#">Integrate a Visual C++ Application.</a> <a href="#">Integrate a C#.NET Application using IIS Application Server.</a>
Visual Basic Script JavaScript	cspmclientatl64.dll See <a href="#">Integrate Windows Applications and Scripts Using a Windows DLL</a> .	<a href="#">Integrate a Visual Basic, Java, or Windows Script.</a>

## Integrate Applications Using Java

Use the `CSPMClient` Java class when integrating a Java application or an application that can launch external Java applications. Add the following reference to the classpath of the requesting application: `$CSPM_CLIENT_HOME/lib/CSPMClient.jar`. The requesting application creates an instance of the `CSPMClient` class when it is required.

### Java Integration Proces

The A2A Client requires OpenJDK Temurin Java 17.

#### Follow these steps:

1. Add the `CSPMClient.jar` file to your classpath. The file is located in `$CSPM_CLIENT_HOME/lib`.
2. Set the path of the folder containing the client configuration file. For UNIX and Windows, set the `CSPM_CLIENT_HOME` environment variable. This path is the location of the client installation directory.
  - UNIX example:  
`-Dcspm_client_config_file=$CSPM_CLIENT_HOME/config/cspm_client_config.xml`
  - Windows example:  
`-Dcspm_client_config_file=%CSPM_CLIENT_HOME%\config\cspm_client_config.xml`
3. If no `CSPM_CLIENT_HOME` value is set, use the current option in the Java command-line option to specify the file location. If no value is specified, use the default installation location values for `CSPM_CLIENT_HOME`.
  - For UNIX, use `/opt/cloakware`
  - For Windows, use `c:\cspm\cloakware`
4. Modify your source code to call the `CSPMClient` class as in [Integrate a Basic Java Application](#):
  - a. Add import classes: `import com.ca.pam.a2a.client.CSPMClient.`
  - b. Instantiate the `CSPMClient.class`.
  - c. Call `retrieveCredentials` to retrieve the credentials.
5. Add the requestor to Credential Manager. See [Add A2A Requestors](#).
6. Add authorization mapping to Credential Manager. See [Add A2A Authorization Mappings](#).

### CSPMClient and Related Java Classes

The `cwjcafips` and `cwjsssefips` classes do not have any methods that you can use but they are dependencies of the `CSPMClient` class. The following table lists the methods that are available from the `(com.ca.pam.a2a.client.CSPMClient)` Java class.

Method	Description
<code>CSPMClient()</code>	Constructor. Takes no parameters.
<code>void retrieveCredentials(String targetAlias)</code>	Retrieves the credentials (account name and password) for the given target alias. Takes one parameter: <ul style="list-style-type: none"> <li>• <code>target alias</code> of type <code>java.lang.String</code>.</li> </ul>

<code>void retrieveCredentials(String targetAlias, String bypassCacheFlag)</code>	Retrieves the credentials (account name and password) for the given target alias. Takes the following parameters: <ul style="list-style-type: none"> <li>target alias of type <code>java.lang.String</code></li> <li>bypass cache flag (either <code>true</code> or <code>false</code>)</li> </ul> If the bypass cache flag is set to <code>true</code> , the local cache is bypassed and the query goes directly to the Credential Manager Server.
<code>void retrieveCredentials(String targetAlias, String bypassCacheFlag, String xmlOutput)</code>	Retrieves the credentials (account name and password) for the given target alias. Takes the following parameters: <ul style="list-style-type: none"> <li>target alias of type <code>java.lang.String</code></li> <li>bypass cache flag (either <code>true</code> or <code>false</code>)</li> <li>(Optional) String <code>xmlOutput</code>. Specify <code>-x</code> to retrieve the output as an XML data string.</li> </ul> If the flag is set to <code>true</code> , the local cache is bypassed and the query goes directly to the Credential Manager Server.
<code>String getUserId()</code>	Returns the account name from the last <code>retrieveCredentials</code> call.
<code>String getPassword()</code>	Returns the password from the last <code>retrieveCredentials</code> call.
<code>String getStatusCode()</code>	Returns the <code>statusCode</code> of type <code>String</code> from the last <code>retrieveCredentials</code> call. For code definitions, see <a href="#">Return Data</a> .
<code>String getMessages()</code>	Returns any error messages.
<code>String getXMLData()</code>	Gets the data from the last <code>retrieveCredentials</code> invocation. Specify <code>-x</code> to retrieve the output as an XML data string.

### Integrate Applications Using the A2A Client

Use the A2A Client (`cspmclient`, `cspmclient64`, `cspmclient.exe`, or `cspmclient64.exe`) when integrating with a non-Java application. The requestor launches the A2A Client. Typically, you integrate an application using the A2A Client (`cspmclient`, `cspmclient64`, `cspmclient.exe`, or `cspmclient64.exe`) when the requestor is:

- Written in C
- Written in C++ or C# and you do not want to use a COM component
- Using a scripting language such as Perl or PowerShell

#### NOTE

Do not call the `cspmclient`, `cspmclient64`, `cspmclient.exe`, or `cspmclient64.exe` interfaces directly from the command line. A requestor calls the interfaces. The requestor cannot be a Bourne shell script, but the requestor can be a Korn shell script.

### A2A Client Integration Process

Use the following process to integrate an application using the A2A Client (`cspmclient`, `cspmclient64`, `cspmclient.exe`, or `cspmclient64.exe`):

- Set up environment variables.  
You can add the A2A Client to the `PATH` variable to avoid hardcoding the path of the A2A Client application.
- Modify your application:
  - For UNIX or Linux, call `cspmclient` or `cspmclient64` to retrieve credentials. For Windows, call `cspmclient.exe` or `cspmclient64.exe`.
  - Read standard output to get the return codes generated by the A2A Client. For code definitions, see [Return Data](#).
- Add the requestor to Credential Manager. See [Add A2A Requestors](#).
- Add authorization mapping to Credential Manager. See [Add A2A Authorization Mappings](#).

### ***cspmclient Constraints***

The default return value is space-delimited. As a result, account names and passwords cannot contain spaces. The string `null` is reserved. Account names and passwords cannot be the string `null`.

### ***cspmclient Usage***

For UNIX or Linux, use one of the following commands:

- For the 32-bit Client: `cspmclient targetAlias [bypassCacheFlag] [-b] [-x]`
- For the 64-bit Client: `cspmclient64 targetAlias [bypassCacheFlag] [-b] [-x]`

For Windows, use the following commands:

- For the 32-bit Client: `cspmclient.exe targetAlias [bypassCacheFlag] [-b] [-x]`
- For the 64-bit Client: `cspmclient64.exe targetAlias [bypassCacheFlag] [-b] [-x]`

Parameter	Description
String <code>targetAlias</code>	Predefined target account alias, which is used to retrieve the account credentials (user name and password).
String <code>bypassCacheFlag</code>	Specifying <code>true</code> directs the A2A Client to bypass the local cache and retrieve account credentials directly from the Credential Manager Server. The default is <code>false</code> .
<code>-b</code>	Short form option for setting <code>bypassCacheFlag</code> to <code>true</code> .
<code>-x</code>	Specifies to return output as an XML data string.

### ***cspmclient Return Values***

The `cspmclient`, `cspmclient64`, `cspmclient.exe` and `cspmclient64.exe` interfaces return the return code, `userID`, and password as a space-delimited string.

Return Value	Description
Return Code	Contains an integer value. See <a href="#">Return Data</a> .
UserID	Contains the account name. If the attempt was unsuccessful, the account name is set to the string <code>null</code> .
Password	Contains the account password. If the attempt was unsuccessful, the password is set to the string <code>null</code> .
message	Contains the error messages text string. If the attempt was unsuccessful, the message text of the associated errors is returned.

### **Integrate Windows Applications and Scripts Using a Windows DLL**

Use Windows Dynamic Link Library (DLL) to integrate a Windows application or a Windows client script that supports COM components. Credential Manager provides the following DLLs:

- Microsoft Foundation Class (MFC) DLL(`cspmclientc.dll` or `cspmclientc64.dll`). The Credential Manager MFC DLL works with applications that are written with Visual Basic or in C, C++, or C#. You cannot use the MFC DLL with scripts.
- Active Template Library (ATL) DLL(`cspmclientatl.dll` or `cspmclientatl64.dll`). The Credential Manager ATL DLL works with .NET applications and supports Visual Basic script and JavaScript.

Both Credential Manager DLLs are COM components. These DLLs allow linking to Windows applications and Windows client scripts that support COM DLLs. The application or script should create an instance of the COM component when it is required. The Windows DLLs are thread-safe if they are not used as a singleton.

### MFC DLL Integration Process

The integration process varies depending on the language that is used to write the application. The following process is a typical way to integrate a C++ application using the Credential Manager MFC DLL:

1. Import the Type Library file (TLB) by adding the following statements in your code: `#import "$CSPM_CLIENT_HOME/cspmclient/lib/cspmclientc.tlb" named_guids using namespace Cspmclientc; .The#import` directive incorporates the information from the type library. The content of the type library is converted into C++ classes to allow you to create the COM component. The `named_guids` argument creates the CLSID and IID to use in `CoCreateInstance`.
2. Create the COM component:  

```

Iccspmclientc *icspmClient = NULL; HRESULT hr = CoCreateInstance(CLSID_ccspmclientc, NULL,
    CLSCTX_INPROC_SERVER, DIID_Iccspmclientc, (void**) &icspmClient );

```
3. Call the `retrieveCredentials` method to retrieve the credentials for a given class. The following call is an example: `long retValue = icspmClient->retrieveCredentials("alias", "true", "");`
4. Add the requestor to Credential Manager. See [Add A2A Requestors](#).
5. Add authorization mapping to Credential Manager. See [Add A2A Authorization Mappings](#).

### ATL DLL Integration Process

The integration process varies depending on the scripting language. For examples, refer to [Integrate a Script](#).

### DLL Methods

The following methods are available from the Credential Manager MFC DLL and the Credential Manager ATL DLL.

Method	Description
<code>long retrieveCredentials(String targetAlias, String bypassCacheFlag, String xmlOutput)</code>	Retrieves the credentials (account name and password) for the given target alias. Returns the <code>statusCode</code> of the <code>getCredentials</code> call. Takes the following parameters: <ul style="list-style-type: none"> <li>• <code>String targetAlias</code> . The predefined target account alias, which is used to retrieve the account credentials (account name and password).</li> <li>• <code>String bypassCacheFlag</code> . Specify <code>true</code> to indicate that the credential should be retrieved from the Credential Manager Server. Specify <code>false</code> to retrieve the credential from the local cache.</li> <li>• (Optional) <code>String xmlOutput</code> . Specify <code>-x</code> to retrieve the output as an XML data string.</li> </ul>
<code>String getUserID()</code>	Returns the account name from the last <code>retrieveCredentials</code> call.
<code>String getPassword()</code>	Returns the password from the last <code>retrieveCredentials</code> call.
<code>String getXMLData()</code>	Gets the data from the last <code>retrieveCredentials</code> call.
<code>String getMessage()</code>	Gets the error message from the last <code>retrieveCredentials</code> call.

### DLL Constraints

Both Credential Manager Windows DLLs are only available for Windows platforms.

## A2A Integration Return Data

Each of the integration methods provides two ways to receive return data—string-based or XML-based. The default behavior returns the return code, account name, and password as strings. Optionally, you can request that the return data be formatted as an XML string.

### XML Return Schema

When you request an XML return string, the following schema is used:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="credential">
    <xs:complexType>
      <xs:all>
        <xs:element name="TargetAlias" type="xs:string"/>
        <xs:element name="TargetAccount" type="xs:string"/>
        <xs:element name="TargetApplication" type="xs:string"/>
        <xs:element name="TargetServer" type="xs:string"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:element name="requestresult">
    <xs:complexType>
      <xs:all>
        <xs:element name="errorcode" type="xs:string"/>
        <xs:element name="errormessage" type="xs:string"/>
        <xs:element name="credential"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:element name="TargetAlias"/>
  <xs:element name="TargetAccount"/>
  <xs:element name="TargetApplication"/>
  <xs:element name="TargetServer"/>
</xs:schema>
```

### NOTE

When you use target connectors, there might be extra extended attributes that are defined within the target connector. The extended attributes are also returned in the XML return string. The schema that is used for these additional elements is defined in the configuration file for the specific target connector.

### XML Return Example

The following XML code is an example of an XML return string:

```
<?xml version="1.0" encoding="utf-8" ?>
<requestresult>
  <errorcode>400</errorcode>
  <errormessage>Success</errormessage>
  <credential>
```



```

<TargetAlias>
<ID>1</ID>
<createDate>Thu Jun 07 12:18:52 EDT 2008</createDate>
<updateDate>Thu Jun 07 12:18:52 EDT 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>Ph6g7JFExM30gT5pGvW965bKCQ0=</hash>
<name>test</name>
<accountID>1</accountID>
</TargetAlias>
<TargetAccount>
<Attribute.descriptor2 />
<Attribute.descriptor1>desc</Attribute.descriptor1>
<ID>1</ID>
<createDate>Tue May 29 11:28:41 EDT 2007</createDate>
<updateDate>Fri Jun 08 15:20:42 EDT 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>R7n+cRYTppkycxWfJiasOZGHNhI=</hash>
<targetApplicationID>1</targetApplicationID>
<userName>testaccount</userName>
<password>W8H8U06H4saHxUo4</password>
<accessType>readwrite</accessType>
<cacheBehavior>noCache</cacheBehavior>
<cacheDuration>30</cacheDuration>
<privileged>false</privileged>
<synchronize>false</synchronize>
<passwordVerified>false</passwordVerified>
<lastVerified>2007-06-08 15:20:42.0</lastVerified>
</TargetAccount>
<TargetApplication>
<Attribute.descriptor2 />
<Attribute.descriptor1 />
<ID>1</ID>
<createDate>Tue May 29 11:25:50 EDT 2007</createDate>
<updateDate>Tue May 29 11:25:50 EDT 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>ylAVs174hPLzqfw142NsGnTsJfM=</hash>
<targetServerID>1</targetServerID>
<type>Generic</type>
<name>testapp</name>
<policyID>0</policyID>
</TargetApplication>
<TargetServer>
<Attribute.descriptor2 />
<Attribute.descriptor1 />
<ID>1</ID>
<createDate>Thu Jun 07 12:14:26 EDT 2007</createDate>
<updateDate>Thu Jun 07 12:14:26 EDT 2007</updateDate>
<createUser>admin</createUser>
<updateUser>admin</updateUser>
<hash>Od4/9x1iVS+1yefQOGbe8BdbxVk=</hash>

```

```
<hostName>testtest</hostName>
<ipAddress />
</TargetServer>
</credential>
</requestresult>
```

## Integrate Java Applications with the Credential Manager A2A Client

This content in this section how to integrate Java applications with the A2A Client to use Credential Manager to retrieve target account credentials.

Use the table of contents to access the topics in this section.

### Integrate a Basic Java Application with the A2A Client

This content describes how to integrate a basic Java application with the A2A Client.

[Install the A2A client](#) on each system where a Java application is to be integrated.

The following example files are provided:

- **Example.java**  
Compile this java class source file to use it.
- **Run\_example**  
This file is a shell script executable. This script requires that you compile the source file. When compiling the source file, use this script for information about how to define the class path.

If you install an A2A Client on a UNIX system, copies of the example files are in the directory `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples`.

#### NOTE

A2A is referred to as **CSPM** in code samples, file, and environment variable names.

#### Example.java Code

```
/*
 * An example class to demonstrate calling the CSPMClient class.
 *
 * Note:
 *
 * You will need to ensure that the library path to the cspm library directory
 * is set by one of the following methods:
 *
 * a. Adding /opt/catech/cspmclient/lib to LD_LIBRARY_PATH, or
 *
 * b. Passing the following option on the java command line:
 *    -Djava.library.path=/opt/catech/cspmclient/lib
 */

public class Example {

    /**
     * Main entry point.
     *
     * @param args[0], String target alias
     */
}
```

```

* @param args[1], bypass cache flag. If set to:
*
*   "true", the cspm client will call the cspm server system
*
*   "false", the cspm client will 1st search the local cache
* @param args[2], xmlOption. (Optional) If set to:
*
*   "-x", Gives the XML data.
* @return int 0 if successful, 100 if an exception occurred, otherwise
* documented error codes for the CSPMClient class.
*
*/

public static void main(String[] args) {

    try {
        //check the arguments
        if(args.length != 2) {
            System.out.println("Missing CLI arguments");
            System.exit(256);
        }
        //initialize
        String targetAlias = args[0];
        String bypassCache = args[1];
String xmlOption= args[2];

        CSPMClient testInterface = new CSPMClient();

If(args.length>2){
xmlOption=args[2];
        testInterface.retrieveCredentials(targetAlias, bypassCache, xmlOption);
}else{

        //get the result
        String statusCode = testInterface.getStatusCode();
        String userId      = testInterface.getUserId();
        String password    = testInterface.getPassword();
String xmlData      = testInterface.getXMLData();

        System.out.println("Status Code: " + statusCode);
        System.out.println("UsedId:      " + userId);
        System.out.println("Password:   " + password);
        System.out.println("XML Data:    " + XmlData);

        //set the return value
        if ( statusCode.equals("400") ) {
            System.out.println("PASSED");
            System.exit(0);
        } else {
            System.out.println("FAILED");
            System.exit(Integer.parseInt(statusCode));
        }
    }
}

```

```

        } catch (Exception e) {
            e.printStackTrace();
            System.exit(100);
        }
    }
}

```

### **Run\_example Code**

The `Run_example` shell script calls `Example.class`. When executing the Java call, the `-D` option sets system property values that are used by the executing program as follows:

- `-Djava.library.path`. This option sets the Java library path; that is, the location of the `$CSPM_CLIENT_HOME/cspmclient/lib` directory. This option can also be set with the environment variable `LD_LIBRARY_PATH` (LIBPATH on AIX).
- `-Dcspm_client_config_file`. This option specifies the client configuration file directory. Use this file if the configuration file is in a non-standard location (that is, not in `/opt`).

```

#!/bin/sh
# This is an EXAMPLE script making use of Example.class in the same directory.
#
# All 2 Run_example CLI arguments are MANDATORY!
# Validate the command line parameters
if [ ! $# = 2 ]
then
    echo " "
    echo " syntax: $0 target_alias bypass_cache"
    echo
    exit 1
fi
# Setup Global Variables
CLASS_NAME=Example
CONFIG_FILE=/opt/cloakware/cspmclient/config/cspm_client_config.xml
JAVA_BINDIR=/opt/cloakware/cspmclient_thirdparty/java/bin
LIB=/opt/cloakware/cspmclient/lib
LOCAL_DIR=`pwd`;
CLASS_PATH=/opt/cloakware/cspmclient/lib/cspmclient.jar:$LOCAL_DIR
#Execute JAVA class
$JAVA_BINDIR/java -classpath $CLASS_PATH -Djava.library.path=$LIB \
-Dcspm_client_config_file=$CONFIG_FILE $CLASS_NAME $1 $2

```

### **Basic Java Integration with Database Connection**

Your installed A2A Client does not contain a soft copy of the following script.

```

/**
 * A sample java class to connect to a database.
 */
import java.sql.*;

import com.cloakware.cspm.client.CSPMClient;

public class DBConnect {

```

---

```

private int LOGIN_FAILED_CODE = 2003;
private String URL = "jdbc:mysql://host:port/database?autoReconnect=true";
private String DRIVER_CLASS = "com.mysql.jdbc.Driver";
// private String userID = "scott";
// private String password = "tiger";

private String TARGET_ALIAS = "TestAccount";
private CSPMClient cspmClient;
// ....
/**
 * Initialize credentials attribute and retrieve the credentials.
 */

private void initialize() {
    cspmClient = new CSPMClient ();
    cspmClient.retrieveCredentials( TARGET_ALIAS );
}

private Connection getConnection() {
    Driver driver = null;
    Connection connection = null;

    // check for initialization
    if ( cspmClient == null ) initialize();

    // check for system error
    if ( !cspmClient.getStatusCode().equals( "400" ) ) {

        // do some error handling.
    }

    try {
        Class.forName(DRIVER_CLASS);
        connection = DriverManager.getConnection( URL
  , cspmClient.getUserId()
  , cspmClient.getPassword() );
    } catch ( ClassNotFoundException ce ) {
        // ....
    } catch ( SQLException e ) {

        // DOUBLE PASS CHECK (OPTIONAL)
        // check for login failed
        if ( e.getErrorCode() == LOGIN_FAILED_CODE ) {
            // try again, bypass Password Authority cache, go directly to Password Authority server
            cspmClient.retrieveCredentials( TARGET_ALIAS, "true" );
            if ( !cspmClient.getStatusCode().equals( "400" ) ) {
                // do some error handling.
            }
            try {

```

```

        connection = DriverManager.getConnection( URL
  , cspmClient.getUserId()
  , cspmClient.getPassword());
    } catch ( SQLException e2 ) {
        // do stuff
    }
}
}
return connection;
}
// ....
}

```

### Register Requestor - Basic Java Application

See [Install and Activate an A2A Client on a Request Server](#) for the procedure to register your requestor with Credential Manager. You need the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension. Example: Run\_example
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type. Example: Java

When entering the file and execution paths, specify the absolute paths without links.

### Integrate a Standalone Java Application Using the A2A Client JDBC Wrapper

This content provides a description of how to use the A2A Client JDBC wrapper in a standalone Java application using the provided example application code as a model.

#### NOTE

For historical reasons, A2A is referred to as CSPM in code samples, file, and environment variable names.

The following line shows the pattern for the connection URL:

```
cspm:URL;CSPMDriver=target_driver;CSPMAlias=alias:
```

- *URL* specifies the usual vendor-specific JDBC URL
- *target\_driver* specifies the classname of the JDBC driver
- *alias* specifies the target alias representing the credentials to use when connecting

In the provided example, the connection URL, which shows a connection to a MySQL database cspm on host milocspm.cloakware.com using the MySQL driver and alias jdbcdemo , is:

```
Cspm:jdbc:mysql://milocspm.cloakware.com:3306/
cspm;CSPMDriver=com.mysql.jdbc.Driver;CSPMAlias=jdbcdemo
```

To obtain the required A2A Client files, [Install the A2A Client](#).

To compile the application, use the `cspmclient.jar` and `cloakwareJdbc.jar` files that are included with the A2A client.

To execute the application, use the previously mentioned JAR files and the vendor-specific JDBC driver JAR file, which in this case is `mysql-connector-java-5.1.8-bin.jar` because the connection is to a MySQL database.

When executing the application, identify the location of the client configuration file, `cspm_client_config.xml`, by specifying the following JVM option:

```
-Dcspm_client_config_file=<path>/cspm_client_config.xml
```

Identify the directory where the native code libraries reside by specifying the following JVM option:

```
-Djava.library.path=<path>/cloakware/cspmclient/lib
```

### **Application Code**

```
package com.cloakware.ps.jdbcdemo;

import java.sql.*;

public class JdbcDemoApp {
    private static final String
    JDBC_DRIVER_CLASS_NAME = "com.cloakware.jdbc.JdbcDriver";
    private static final String
    JDBC_URL = "cspm:jdbc:mysql://milocspm.cloakware.com:3306/
    cspm;CSPMDriver=com.mysql.jdbc.Driver;CSPMAlias=jdbcdemo";

    private Connection m_connection = null;

    public JdbcDemoApp() {

    try {

        System.out.println( "instantiating the JDBC driver" );

        Class.forName( JDBC_DRIVER_CLASS_NAME ).newInstance();

        System.out.println( "invoking the driver to obtain a connection to the database" );

        m_connection = DriverManager.getConnection( JDBC_URL );

        runDemo();

    } catch ( Exception ex ) {

        ex.printStackTrace();

    } finally {

        try {
```

```

if ( m_connection != null )
m_connection.close();
} catch ( SQLException ex ) {
}

}

}

private void runDemo() {

final String QUERY = "select count(*) from init_properties;";

try {
System.out.println( "executing query" );

Statement st = m_connection.createStatement();
ResultSet rs = st.executeQuery( QUERY );

while ( rs.next() ) {
System.out.println( "result= " + rs.getInt( 1 ) );
}

} catch ( SQLException ex ) {
ex.printStackTrace();
}

}

public static void main(String[] args) {

new JdbcDemoApp();

}

}

```

## Integrate a Java Application with the A2A Client on JBoss

This content describes an example that uses the A2A Client to manage the credentials that are used by a Java container JDBC connection pool within a JBoss application server version 4.2.2.

### NOTE

For historical reasons, A2A is referred to as CSPM in code samples, file, and environment variable names.

This example uses a credential viewer and an HSQLDB data store to show the following functionality:

- The credential viewer shows you how to view credentials that are stored in the Credential Manager server using the CSPMClient Java class. Use this example for simple integration and to test the ability to connect to Credential Manager and retrieve credentials. The example displays the credentials to the screen.
- The HSQLDB data store shows you how to configure a data store using the Credential Manager JdbcDriver Java class to retrieve credentials and connect to an HSQLDB data store. The example retrieves credentials and uses them to access a data store.



This example is available on all A2A Client installations in the following directories, for:

- **UNIX:** `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/JBoss_Sample`
- **Windows:** `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/JBoss_Sample`

File	Description
<code>ClassFactory.java</code>	Class factory that is used to create the objects that are used in the example web application. The class allows you to create the <code>CSPMClient</code> class and to perform a lookup in the Initial Context to retrieve the data source that is used to get a connection to the database.
<code>CredentialsViewer.java</code>	Servlet class that is used to connect to the Credential Manager server to retrieve credentials.
<code>ConnectionTester.java</code>	Servlet class that is used to create 10 connections to a database and execute a basic SQL statement. The class retrieves the <code>DataSource</code> class using the <code>ClassFactory</code> class.
<code>cspm_connect_hsql_org-ds.xml</code>	Configuration file showing how to configure a data source using the HSQLDB driver.
<code>cspm_connect_hsql-ds.xml</code>	Configuration file showing how to configure a data source using the Credential Manager <code>JdbcDriver</code> . The target driver is HSQLDB.

### **Integration Process for JBoss**

Use the following process to modify your application to use the Credential Manager server to manage credentials:

1. Configure the development environment. See [Configure your Development Environment for JBoss](#).
2. Optionally, integrate the A2A Client to retrieve credentials. See [JBoss Credential Viewer](#).
3. Create or modify the data source file. See [JBoss Connection Pool with HSQLDB Data Store](#).
4. Register requestor. See [Register JBoss Requestor](#).

### **Configure Your Development Environment for JBoss**

Configure your development environment for both JBoss development and Credential Manager integration.

The example contains an Apache ANT build file that is located in the build directory that you can use to create the WAR file and to deploy it. The build file is compatible with ANT 1.6.5 and above.

#### ***Configure Your Environment for JBoss Development***

Use the following procedure to configure your environment for JBoss development.

#### **Follow these steps:**

1. Install JBoss Application Server 4.2.2 GA. See <http://sourceforge.net/projects/jboss/files/JBoss/JBoss-4.2.2.GA>.
2. Set the `JBOSS_HOME` environment variable. See [https://docs.jboss.org/jbossas/docs/Installation\\_And\\_Getting\\_Started\\_Guide/5/html/setting\\_JBOSS\\_HOME.html](https://docs.jboss.org/jbossas/docs/Installation_And_Getting_Started_Guide/5/html/setting_JBOSS_HOME.html).
3. Install Apache ANT 1.6.5 or above. See <http://ant.apache.org/bindownload.cgi>.
4. Set the `ANT_HOME` environment variable. See <http://ant.apache.org/manual/install.html>.
5. Install the Java Database HSQLDB 1.8.0. See [http://sourceforge.net/project/showfiles.php?group\\_id=23316](http://sourceforge.net/project/showfiles.php?group_id=23316).
6. Set the `HSQL_HOME` environment variable to the path where you installed HSQL (for example, `opt/tools/hsqldb`).

#### ***Configure Your Environment for A2A Client Integration with JBoss***

Use the following procedure to configure your environment for A2A Client integration with JBoss.

**Follow these steps:**

1. **Install** the A2A Client
2. Create or add to the JAVA\_OPTS environment variable:
  - UNIX:
    - Djava.library.path=\$CSPM\_CLIENT\_HOME\lib
    - Dcspm\_client\_config\_file=\$CSPM\_CLIENT\_HOME\config\cspm\_client\_config.xml
  - Windows:
    - Djava.library.path=%CSPM\_CLIENT\_HOME%\lib
    - Dcspm\_client\_config\_file=%CSPM\_CLIENT\_HOME%\config\cspm\_client\_config.xml
3. Copy the `cloakwareJdbc.jar` file that is located in the A2A Client `tools` directory to the Jboss default deployment directory:
  - UNIX:
    - Source: \$CSPM\_CLIENT\_HOME/cspmclient/tools
    - Destination: \$JBASS\_HOME/server/default/lib
  - Windows:
    - Source: %CSPM\_CLIENT\_HOME%/cspmclient/tools
    - Destination: %JBASS\_HOME%/server/default/lib
4. Copy the `cspmclient.jar` file that is located in the A2A Client `lib` folder to the JBoss default deployment `lib` folder.

**NOTE**

Perform Step 2 and Step 3 using the ANT build file that is located in the following directories:

- UNIX: \$CSPM\_CLIENT\_HOME/examples/java/JBoss\_Sample/build
- Windows: %CSPM\_CLIENT\_HOME%/examples/java/JBoss\_Sample/build

Enter `ant deploy.driver.lib` from that directory.

**Deploy and Run the Sample JBoss Application**

Use the following procedure to compile and run the sample web application using an Apache Ant task.

Follow these steps:

1. Verify that the JBoss application server is running (default configuration).
2. Open a command line window.
3. Navigate to one of the following directories:
  - UNIX: \$CSPM\_CLIENT\_HOME/cloakware/cspmclient/examples/java/JBoss\_Sample/build
  - Windows: %CSPM\_CLIENT\_HOME%/cloakware/cspmclient/examples/java/JBoss\_Sample/build
4. Start the HSQLDB server by entering `ant start.hsqldb`.
5. Compile and deploy the example by entering `ant`.
6. Open a Web Browser.
7. Display the credential viewer web application by loading the following page: `http://localhost:8080/cspmJBossSample`.

**JBoss Credential Viewer**

This example servlet shows you how to use the A2A Client class to retrieve the credentials.

The `CSPMClient` class is created using a class factory.

***Class File***

```
package com.cloakware.cspm.sample.web;
```

```

import java.io.IOException;

import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import com.cloakware.jdbc.StatusCodeMapping;
import com.cloakware.cspm.client.CSPMClient;
import com.cloakware.cspm.sample.ClassFactory;

/**
 * This servlet class is used to retrieve credentials using the
 * CSPMClient class.<br>
 * <br>
 * The user enters a CSPMAlias Name and the servlet displays the information
 * returned by the CSPMClient class. <br>
 * <br>
 * Since the CSPMClient class only returns a status code, the base class
 * provides a class to convert the status code to a more meaningful sentence.
 */
public class CredentialsViewer extends HttpServlet {
    /* Attribute names */
    private final String ERROR_MSG = "errorMsg";

    /* Parameter names and attributes when refreshing the page */
    private final String ALIAS_NAME = "aliasName";
    private final String BYPASS_CACHE = "byPassCache";
    /* Attributes used when displaying credentials/response from
     * the CSPMClient class.
     */
    private final String RETURN_CODE = "returnCode";
    private final String RETURN_MSG = "returnMsg";
    private final String USERNAME = "username";
    private final String PASSWORD = "password";
    /* Error message */
    private final String MSG_ALIAS_EMPTY = "Alias cannot be empty";
    /* Response page */
    private final String TARGET_JSP = "/index.jsp";
    /**
     * Constructor of the object.
     */
    public CredentialsViewer() {
        super();
    }

    /**
     * The doGet method of the servlet. <br>
     *
     * This method is called when a form has its tag value method equals to get.
     * The method retrieves the alias name and the value of the checkbox

```

```

* indicating if the CSPMClient cache needs to be bypassed. It then calls
* the retrieveCredentials method of the CSPMClient class and displays the
* results. An error message is displayed if the alias name is missing.
*
* @param request the request send by the client to the server
* @param response the response send by the server to the client
* @throws ServletException if an error occurred
* @throws IOException if an error occurred
*/
public void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {

    // Retrieve the parameters
    String alias = (String)request.getParameter(ALIAS_NAME);
    Object byPassCache = request.getParameter(BYPASS_CACHE);
    // Make sure to redisplay the alias name.
    request.setAttribute(ALIAS_NAME, alias);
    request.setAttribute(BYPASS_CACHE,
        (byPassCache != null) ? "checked" : null);

    // if we have an alias
    if (alias != null && !"".equals(alias)) {
        // Class used to retrieve the credential.
        CSPMClient cspmClient = ClassFactory.getCSPMClient();

        // Retrieve the credentials.
        if (byPassCache == null) {
            cspmClient.retrieveCredentials(alias);
        } else {
            cspmClient.retrieveCredentials(alias, "true");
        }

        // Set the credentials in the request
        request.removeAttribute(ERROR_MSG);
        request.setAttribute(RETURN_CODE, cspmClient.getStatusCode());
        String statusMsg = StatusCodeMapping
            .getStatusText(cspmClient);
        request.setAttribute(RETURN_MSG, statusMsg);
        request.setAttribute(USERNAME, cspmClient.getUserId());
        request.setAttribute(PASSWORD, cspmClient.getPassword());
    } else {
        // return an error message.
        request.setAttribute(ERROR_MSG, MSG_ALIAS_EMPTY);
        request.removeAttribute(RETURN_CODE);
    }

    // Get the request dispatcher
    RequestDispatcher dispatcher = getServletContext()
        .getRequestDispatcher(TARGET_JSP);

    // Forward to the jsp file to display the credentials
    dispatcher.forward(request, response);
}

```

```
}
```

## **JBoss Connection Pool with HSQLDB Data Store**

This example shows you how to create or modify a data source to use the Credential Manager server for credential retrieval. The data source definitions are saved in files ending with the suffix `-ds.xml` and are located in the deployment folder.

To integrate the A2A Client to your application, change the JDBC driver that is used by the data source. The Credential Manager JDBC driver acts as a proxy JDBC driver serving any JDBC URL that is recognized as a Credential Manager JDBC URL. In the data source configuration, provide information regarding the targeted driver and the alias to use in the special Credential Manager style JDBC URL. The Credential Manager style JDBC URL format is:

```
cspm:[url];CSPMDriver=target.driver;CSPMAlias=alias
```

Form the Credential Manager URL as follows:

- Ensure that it begins with the `cspm:` prefix.
- Follow the prefix with the normal JDBC URL, omitting any user/password specification; for example, `jdbc:hsqldb:hsq://localhost:9001/cspml`.
- Set the URL to contain the `CSPMDriver` that indicates an explicit JDBC driver to use.
- Assign the `CSPMAlias`, which is the alias for the database user in the Credential Manager server, to the URL.

To use the Credential Manager JDBC driver, modify attributes in the configuration file.

### **Follow these steps:**

1. Set `connection-url` as specified previously.
2. Set `driver-class` to `com.cloakware.jdbc.JdbcDriver`.

This low-level driver management for connection acquisition means that all new connections that are obtained for a user whose database password has been changed (by the Credential Manager server) are made using the new password. This action occurs automatically without any knowledge or intervention by any owning data source.

While new connections are obtained using the new password, old connections that were obtained using an old password can linger in the data source pool. Also, if the Credential Manager alias is changed to a new user, then a connection pool has (at least temporarily) a mixture of connections for different actual database users.

Such connection management by the CA Technologies driver ensures that database password changes are transparent to the activities of the data source.

The XML file that is used in the example is located in one of the following locations:

- **UNIX:** `$CSPM_CLIENT_HOME/cspmclient/examples/java/JBoss_Sample/main/resources/datasources`
- **Windows:** `%CSPM_CLIENT_HOME%/cspmclient/examples/java/JBoss_Sample/main/resources/datasources`

### **Data Source**

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- The Hypersonic embedded database JCA connection factory config -->
<datasources>
<local-tx-datasource>

<!-- The jndi name of the DataSource, it is prefixed with java:/ -->
<jndi-name>jdbc/CSPMSampleDS</jndi-name>

<connection-url>
```

```

cspm:jdbc:hsqldb:hsqldb://localhost:9001/cspm1;
CSPMAlias=hsqldb;CSPMDriver=org.hsqldb.jdbcDriver
</connection-url>

<!-- The driver class -->
<driver-class>com.cloakware.jdbc.JdbcDriver</driver-class>

<!-- The login and password -->
<user-name></user-name>
<password></password>

<!-- The minimum connections in a pool/sub-pool. -->
<min-pool-size>5</min-pool-size>

<!-- The maximum connections in a pool/sub-pool -->
<max-pool-size>10</max-pool-size>

<!-- The time before an unused connection is destroyed -->
<idle-timeout-minutes>1</idle-timeout-minutes>

<track-statements />

<prepared-statement-cache-size>32</prepared-statement-cache-size>

<!-- corresponding type-mapping in the standardjbosscomp-jdbc.xml -->
<metadata>
<type-mapping>Hypersonic SQL</type-mapping>
</metadata>

</local-tx-datasource>
</datasources>

```

### **Register JBoss Requestor**

See [Install and Activate an A2A Client on a Request Server](#) for the procedure to register your requestor with Credential Manager. Use the following data.

Parameter	Description
Script Name	com.cloakware.cspm.sample.web.CredentialsViewer
Execution Path	C:\jboss-4.2.2.GA\bin
Type	Java

Parameter	Description
Script Name	com.cloakware.client.jdbc.JdbcDriver
Execution Path	C:\jboss-4.2.2.GA\bin
Type	Java

### Register HSQLDB as a Target Application

See [Specify a Target Server](#) for the procedure to register HSQLDB as a target application with Credential Manager. Use the following data.

Parameter	Description
Application Name	HSQLDB Server
Application Type	HSQL
DB Port	9001

Parameter	Description
Application	HSQLDB Server
Account Name	sa
Password	admin
Database Name	cspm1

Parameter	Description
Application	HSQLDB Server
Account Name	TestUser
Password	Test
Database Name	cspm1
A2A Account	selected
Change Process	Select: - Use the following account to change password: SA

Parameter	Description
Targets Alias Name	hsq
Application	HSQLDB Server
Account	TestUser

### Register Mapping Between Request Server and Target Alias

See [Add A2A Authorization Mappings](#) for the procedure to register the mapping between the request server and the target alias. Use the following data.

Parameter	Description
Target Alias	Hsql
Request Server	Select your request server
Script	all

## HSQL Database Usage

HSQldb is an SQL relational database engine that is written in Java. It is used in the example as the database server.

Use the following procedure to start the database server.

### Follow these steps:

1. Open a command line window.
2. Navigate to one of the following directories:
  - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/ApacheTomcat/build`
  - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/ApacheTomcat/build`
3. Start the HSQldb server by entering `ant start.hsldb`.

Use the following procedure to shut down the database server.

### Follow these steps:

1. Open a command line window.
2. Navigate to one of the following directories:
  - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/ApacheTomcat/build`
  - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/ApacheTomcat/build`
3. Shut down the HSQldb server by entering `ant shutdown.hsldb`.

## Integrate a Java Application with the A2A Client on Tomcat

This content describes an example that uses the A2A Client to manage the credentials that are used by a Java container JDBC connection pool within a supported Apache Tomcat Application Server.

This example uses a credential viewer and an HSQldb data store to show the following functionality:

- The credential viewer shows you how to view credentials that are stored in the Credential Manager server using the CSPMClient Java class. Use this example for simple integration and to test the ability to connect to Credential Manager and retrieve credentials. The example displays the credentials to the screen.
- The HSQldb data store shows you how to configure a data store using the Credential Manager JdbcDriver Java class to retrieve credentials and connect to an HSQldb data store. The example retrieves credentials and uses them to access a data store.

### NOTE

For historical reasons, A2A is referred to as CSPM in code samples, file, and environment variable names.

This example is available on all A2A Client installations in one of the following directories:

- UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/Tomcat_Sample`
- Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/Tomcat_Sample`

File	Description
<code>ClassFactory.java</code>	Class factory that is used to create the objects that are used in the example web application. The class allows you to create the CSPMClient class and to perform a lookup in the Initial Context to retrieve the data source that is used to get a connection to the database.
<code>CredentialsViewer.java</code>	Servlet class that is used to connect to the Credential Manager server to retrieve credentials.



ConnectionTester.java	Servlet class that is used to create 10 connections to a database and execute a basic SQL statement. The class retrieves the <code>DataSource</code> class using the <code>ClassFactory</code> class.
context.xml	Configuration file showing you how to configure a database resource using the HSQLDB driver and a second resource using the Credential Manager <code>JdbcDriver</code> Java class.

### **Integration Process for Tomcat**

Use the following process to modify your application to use the Credential Manager server to manage credentials:

1. Configure your development environment. See [Configure your Development Environment for Apache Tomcat](#).
2. Optionally, integrate the A2A Client to retrieve credentials. See [Apache Tomcat Credential Viewer](#).
3. Create or modify the context file. See [Apache Tomcat Connection Pool with HSQLDB Data Store](#).
4. Register the requestor. See [Register Apache Tomcat Requestor](#).

### **Configure Your Development Environment for Apache Tomcat**

Configure your development environment for both Apache Tomcat development and Credential Manager integration.

The example contains an Apache ANT build file that is located in the build directory that you can use to create the WAR file and to deploy it. The build file is compatible with ANT 1.6.5 and above.

#### ***Configure Your Environment for Apache Tomcat development***

Use the following procedure to configure your environment for Apache Tomcat development.

##### **Follow these steps:**

1. Install Apache Tomcat Application Server v5.5. See <http://archive.apache.org/dist/tomcat/tomcat-5>.
2. Install Apache ANT 1.6.5 or above. See <http://ant.apache.org/bindownload.cgi>.
3. Set the `ANT_HOME` environment variable. See <http://ant.apache.org/manual/install.html>.
4. Install the Java Database HSQLDB 1.8.0. See [http://sourceforge.net/project/showfiles.php?group\\_id=23316](http://sourceforge.net/project/showfiles.php?group_id=23316).
5. Set the `HSQL_HOME` environment variable to the path where you installed HSQL (for example, `opt/tools/hsqldb`).

#### ***Configure Your Environment for A2A Client Integration with Apache Tomcat***

Use the following procedure to configure your environment for A2A Client integration with Apache Tomcat.

##### **Follow these steps:**

1. [Install the A2A Client](#).
2. Copy the `cspmclient.jar` file that is located in the A2A Client `lib` directory to the Apache Tomcat Common Lib directory:
  - UNIX:  
Source: `$CSPM_CLIENT_HOME/cloakware/cspmclient/lib`  
Destination: `$APACHE_TOMCAT_HOME/common/lib`
  - Windows:  
Source: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/lib`  
Destination: `%APACHE_TOMCAT_HOME%/common/lib`
3. Copy the `cloakwareJdbc.jar` file that is located in the A2A Client `tools` directory to the Apache Tomcat Common Lib directory:
  - UNIX:  
Source: `$CSPM_CLIENT_HOME/cspmclient/tools`  
Destination: `$APACHE_TOMCAT_HOME/common/lib`
  - Windows:

Source: %CSPM\_CLIENT\_HOME%/cspmclient/tools

Destination: %APACHE\_TOMCAT\_HOME%/common/lib

#### NOTE

Perform Steps 1 and using the ANT build file that is located in the following directories:

- UNIX: \$CSPM\_CLIENT\_HOME/examples/java/Tomcat\_Sample/build
- Windows: %CSPM\_CLIENT\_HOME%/examples/java/Tomcat\_Sample/build

Enter `ant deploy.driver.lib` from that directory.

4. Open the Apache Tomcat Properties dialog.
5. Click the Java tab.
6. Add the following text in the Java Options edit field:

– UNIX:

`-Djava.library.path=$CSPM_CLIENT_HOME\lib`

`-Dcspm_client_config_file=$CSPM_CLIENT_HOME\config\cspm_client_config.xml`

– Windows:

`-Djava.library.path=%CSPM_CLIENT_HOME%\lib`

`-Dcspm_client_config_file=$CSPM_CLIENT_HOME%\config\cspm_client_config.xml`

Substitute `CSPM_CLIENT_HOME` with the install directory of the client (for example, `c:\cloakware\cspmclient`).

7. Restart Apache Tomcat. (Stop and start the service.)

#### NOTE

Perform Step 2 and Step 3 using the ANT build file that is located in the following directories:

- UNIX: \$CSPM\_CLIENT\_HOME/examples/java/Tomcat\_Sample/build
- Windows: %CSPM\_CLIENT\_HOME%/examples/java/Tomcat\_Sample/build

Enter `ant deploy.driver.lib` from that directory.

### Deploy and Run the Sample Tomcat Application

Use the following procedure to compile and deploy the sample web application using an Apache Ant task.

Follow these steps:

1. Verify that Apache Tomcat is running.
2. With a text editor (such as Notepad or Vim), edit the `build.properties` file that is located in the following directories:
  - UNIX: \$CSPM\_CLIENT\_HOME/cloakware/cspmclient/examples/java/Tomcat\_Sample/build
  - Windows: %CSPM\_CLIENT\_HOME%/cloakware/cspmclient/examples/java/Tomcat\_Sample/build
3. Change the value of the `dir.server` property (for example, to `C:/Program Files/Apache Software Foundation/Tomcat 5.5`) and save the file.
4. Open a command line window.
5. Navigate to one of the following directories:
  - UNIX: \$CSPM\_CLIENT\_HOME/cloakware/cspmclient/examples/java/Tomcat\_Sample/build
  - Windows: %CSPM\_CLIENT\_HOME%/cloakware/cspmclient/examples/java/Tomcat\_Sample/build
6. Start the HSQLDB server by entering `ant start.hsqldb`.
7. Compile and deploy the example by entering `ant`.
8. Open a Web Browser.
9. Load the following page: <http://localhost:8088/cspmTomcatSample>.

## **Apache Tomcat Credential Viewer**

This example servlet shows you how to use the `CSPMClient` class to retrieve the credentials.

The `CSPMClient` class is created using a class factory.

### ***Class File***

```
package com.cloakware.cspm.sample.web;

import java.io.IOException;

import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import com.cloakware.jdbc.StatusCodeMapping;
import com.cloakware.cspm.client.CSPMClient;
import com.cloakware.cspm.sample.ClassFactory;

/**
 * This servlet class is used to retrieve credentials using the
 * CSPMClient class.<br>
 * <br>
 * The user enters a CSPMAlias Name and the servlet displays the information
 * returned by the CSPMClient class. <br>
 * <br>
 * Since the CSPMClient class only returns a status code, the base class
 * provides a class to convert the status code to a more meaningful sentence.
 */
public class CredentialsViewer extends HttpServlet {
    /* Attribute names */
    private final String ERROR_MSG = "errorMsg";

    /* Parameter names and attributes when refreshing the page */
    private final String ALIAS_NAME = "aliasName";
    private final String BYPASS_CACHE = "byPassCache";
    /* Attributes used when displaying credentials/response from
     * the CSPMClient class.
     */
    private final String RETURN_CODE = "returnCode";
    private final String RETURN_MSG = "returnMsg";
    private final String USERNAME = "username";
    private final String PASSWORD = "password";
    /* Error message */
    private final String MSG_ALIAS_EMPTY = "Alias cannot be empty";
    /* Response page */
    private final String TARGET_JSP = "/index.jsp";
    /**
     * Constructor of the object.
     */
    public CredentialsViewer() {
        super();
    }
}
```

```

}

/**
 * The doGet method of the servlet. <br>
 *
 * This method is called when a form has its tag value method equals to get.
 * The method retrieves the alias name and the value of the checkbox
 * indicating if the CSPMClient cache needs to be bypassed. It then calls
 * the retrieveCredentials method of the CSPMClient class and displays the
 * results. An error message is displayed if the alias name is missing.
 *
 * @param request the request send by the client to the server
 * @param response the response send by the server to the client
 * @throws ServletException if an error occurred
 * @throws IOException if an error occurred
 */
public void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {

    // Retrieve the parameters
    String alias = (String)request.getParameter(ALIAS_NAME);
    Object byPassCache = request.getParameter(BYPASS_CACHE);
    // Make sure to redisplay the alias name.
    request.setAttribute(ALIAS_NAME, alias);
    request.setAttribute(BYPASS_CACHE,
        (byPassCache != null) ? "checked" : null);

    // if we have an alias
    if (alias != null && !"".equals(alias)) {
        // Class used to retrieve the credential.
        CSPMClient cspmClient = ClassFactory.getCSPMClient();

        // Retrieve the credentials.
        if (byPassCache == null) {
            cspmClient.retrieveCredentials(alias);
        } else {
            cspmClient.retrieveCredentials(alias, "true");
        }

        // Set the credentials in the request
        request.removeAttribute(ERROR_MSG);
        request.setAttribute(RETURN_CODE, cspmClient.getStatusCode());
        String statusMsg = StatusCodeMapping
            .getStatusText(cspmClient);
        request.setAttribute(RETURN_MSG, statusMsg);
        request.setAttribute(USERNAME, cspmClient.getUserId());
        request.setAttribute(PASSWORD, cspmClient.getPassword());
    } else {
        // return an error message.
        request.setAttribute(ERROR_MSG, MSG_ALIAS_EMPTY);
        request.removeAttribute(RETURN_CODE);
    }
}

```

```
// Get the request dispatcher
RequestDispatcher dispatcher = getServletContext()
.getRequestDispatcher(TARGET_JSP);

// Forward to the jsp file to display the credentials
dispatcher.forward(request, response);
}
}
```

### **Apache Tomcat Connection Pool with HSQLDB Data Store**

This example shows you how to create or modify a resource to use the Credential Manager server for credential retrieval. You can add the data source definitions to the `context.xml` file located in the META-INF directory of the WAR file.

To integrate the A2A Client with your application, change the JDBC driver that is used by the data source. The Credential Manager JDBC driver acts as a proxy JDBC driver serving any JDBC URL that is recognized as a Credential Manager JDBC URL. In the data source configuration, provide information regarding the targeted driver and the alias to use in the special Credential Manager style JDBC URL. The Credential Manager style JDBC URL format is:

```
cspm:[url];CSPMDriver=target.driver;CSPMAlias=alias
```

Form the Credential Manager URL as follows:

- Ensure that it begins with the `cspm:` prefix.
- Follow the prefix by the normal JDBC URL, omitting any user/password specification; for example, `jdbc:hsqldb:hsqldb://localhost:9001/cspml`.
- Set the URL to contain the `CSPMDriver` that indicates an explicit JDBC driver to use.
- Assign the `CSPMAlias`, which is the alias for the database user in the Credential Manager server, to the URL.

Use the following procedure to modify to attributes in the configuration file to use the Credential Manager JDBC driver.

Follow these steps:

1. Set `url` as specified previously.
2. Set `driverClassName` to `com.cloakware.jdbc.JdbcDriver`.

This low-level driver management for connection acquisition means that all new connections that are obtained for a user whose database password has been changed (by the Credential Manager server) are made using the new password. This action occurs automatically without any knowledge or intervention by any owning data source.

While new connections are obtained using the new password, old connections that were obtained using an old password might linger in the data source pool. Also, if the CA Technologies alias is changed to a new user, then a connection pool has (at least temporarily) a mixture of connections for different actual database users.

Such connection management by the CA Technologies driver ensures that database password changes are transparent to the activities of the data source.

The XML file that is used in the example is located in the following locations:

- **UNIX:** `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/Tomcat_Sample/main/resources/META-INF`
- **Windows:** `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/Tomcat_Sample/main/resources/META-INF`

### **Data Source**

```
<Context docBase="SampleDataSources">

<Resource name="jdbc/CSPMSampleDS" auth="Container"
```

```

type="javax.sql.DataSource" maxActive="10" maxIdle="5" maxWait="10000"
username="hsqldb" password=""
driverClassName="com.cloakware.jdbc.JdbcDriver"
url="cspm:jdbc:hsqldb:hsqldb://localhost:9001/cspm1;
CSPMAlias=hsqldb;
CSPMDriver=org.hsqldb.jdbcDriver"
removeAbandoned="true"
removeAbandonedTimeout="30"
logAbandoned="true" />
</Context>

```

## Register Apache Tomcat Requestor

See [Add and Run Credential Manager A2A Requestors](#) for the procedure to register your requestor with Credential Manager. Use the following data:

Parameter	Description
Script Name	com.cloakware.cspm.sample.web.CredentialsViewer
Execution Path	C:\Program Files\Apache Software Foundation\Tomcat 5.5\bin
Type	Java

Parameter	Description
Script Name	com.cloakware.client.jdbc.JdbcDriver
Execution Path	C:\Program Files\Apache Software Foundation\Tomcat 5.5\bin
Type	Java

HSQldb is an SQL relational database engine that is written in Java. HSQldb is used in the example as the database server. See also:

- [Register HSQldb as a Target Application](#)
- [Register Mapping between Request Server and Target Alias](#)
- [HSQL Database Usage](#)

## Integrate a Java Application with the A2A Client on WebLogic

This example uses the A2A Client to manage the credentials that are used by a Java container JDBC connection pool within a supported Oracle WebLogic Server. You must [install](#) the A2A Client on each WebLogic server to be integrated..

This example uses a credential viewer and an HSQldb data store to show the following:

- The credential viewer shows you how to view credentials that are stored in the Credential Manager server using the CSPMClient Java class. Use this example for simple integration and to test the ability to connect to Credential Manager and retrieve credentials. The example displays the credentials to the screen.
- The HSQldb data store shows you how to configure a data store using the Credential Manager JdbcDriver Java class to retrieve credentials and connect to an HSQldb data store. The example retrieves credentials and uses them to access a data store.

### NOTE

For historical reasons, A2A is referred to as CSPM in code samples, file, and environment variable names.

This example is available on all A2A Client installations, in the following directories:

- **UNIX:** `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/WebLogic_Sample`
- **Windows:** `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/WebLogic_Sample`

File	Description
<code>ClassFactory.java</code>	Class factory that is used to create the objects that are used in the example Web application. The class allows you to create the <code>CSPMClient</code> class and to perform a lookup in the Initial Context to retrieve the data source used to get a connection to the database.
<code>CredentialsViewer.java</code>	Servlet class used to connect to the Credential Manager server to retrieve credentials.
<code>ConnectionTester.java</code>	Servlet class used to create 10 connections to a database and execute a basic SQL statement. The class retrieves the <code>DataSource</code> class using the <code>ClassFactory</code> class.

### Integration Process for WebLogic

Use the following process to modify your application to use the Credential Manager server to manage credentials:

1. Configure development environment. See [Configure your Development Environment for WebLogic](#)
2. Optionally, integrate the A2A Client to retrieve credentials. See [WebLogic Credential Viewer](#).
3. Create or modify the data source file. See [WebLogic Connection Pool with HSQLDB Data Store](#).
4. Register the requestor. See [Register WebLogic Requestor](#).

### Configure your Development Environment for WebLogic

You must configure your development environment for both WebLogic development and Credential Manager integration.

The example contains an Apache ANT build file located in the `build` directory that you can use to create the WAR file and to deploy it. The build file is compatible with ANT 1.6.5 and above.

Use the following procedure to configure your environment for WebLogic development.

#### Follow these steps:

1. Install WebLogic Server 10.0. See <http://www.oracle.com/technetwork/middleware/ias/downloads/101310-085449.html>.
2. With the WebLogic Configuration Wizard application, create a domain called `cspmSample` using the default settings. Consult the WebLogic documentation for further assistance.
3. Install Apache ANT 1.6.5 or above. See <http://ant.apache.org/bindownload.cgi>.
4. Set the `ANT_HOME` environment variable. See <http://ant.apache.org/manual/install.html>.
5. Install the Java Database HSQLDB 1.8.0. See [http://sourceforge.net/project/showfiles.php?group\\_id=23316](http://sourceforge.net/project/showfiles.php?group_id=23316).
6. Set the `HSQL_HOME` environment variable to the path where you installed HSQL (for example, `opt/tools/hsqldb`).

Use the following process to configure your environment for A2A Client integration with WebLogic.

#### Follow these steps:

1. Create or add to the `JAVA_OPTIONS` environment variable:
  - UNIX:
    - Djava.library.path=\$CSPM\_CLIENT\_HOME\lib
    - Dcspm\_client\_config\_file=\$CSPM\_CLIENT\_HOME\config\cspm\_client\_config.xml
  - Windows:
    - Djava.library.path=%CSPM\_CLIENT\_HOME%\lib
    - Dcspm\_client\_config\_file=%CSPM\_CLIENT\_HOME%\config\cspm\_client\_config.xml

2. Copy the `cspmclient.jar` file located in the A2A Client `lib` directory to the `lib` directory for your WebLogic domain:
  - UNIX:
    - Source: `$CSPM_CLIENT_HOME/cloakware/cspmclient/lib`
    - Destination: `$WEBLOGIC_HOME/user_projects/domains/$YOUR_DOMAIN/lib`
  - Windows:
    - Source: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/lib`
    - Destination: `%WEBLOGIC_HOME%/user_projects/domains/%YOUR_DOMAIN%/lib`
3. Copy the `cloakwareJdbc.jar` file located in the A2A Client `tools` directory to the WebLogic home directory:
  - UNIX:
    - Source: `$CSPM_CLIENT_HOME/cspmclient/tools`
    - Destination: `$WEBLOGIC_HOME/user_projects/domains/$YOUR_DOMAIN/lib`
  - Windows:
    - Source: `%CSPM_CLIENT_HOME%/cspmclient/tools`
    - Destination: `%WEBLOGIC_HOME%/user_projects/domains/%YOUR_DOMAIN%/lib`

Step 1 and Step 2 are performed by the ANT build file located in the following directories:

- UNIX: `$CSPM_CLIENT_HOME/examples/java/WebLogic_Sample/build`
- Windows: `%CSPM_CLIENT_HOME%/examples/java/WebLogic_Sample/build`

Enter `ant deploy.driver.lib` from that directory.

### **Deploy and Run the Sample WebLogic Application**

Use the following procedure to compile and run the sample web application using an Apache Ant task.

#### **Follow these steps:**

1. Make sure WebLogic is running and using the domain that you created in [Configure your Development Environment for WebLogic](#).
2. With a text editor (such as NotePad or Vim), edit the `build.properties` file located in the following locations, for:
  - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/WebLogic_Sample/build`
  - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/WebLogic_Sample/build`
3. Change the value of the following properties and save the file:
  - `dir.bea`. Points to the location where Bea WebLogic Server 10.0 is installed (for example, `C:/bea` )
  - `weblogic.adminurl`. Administration console URL (for example, `t3://localhost:7001` )
  - `weblogic.domain`. WebLogic domain to use for the deployment. This should match the `cspmSample` domain name that you created in [Configure your Development Environment for WebLogic](#).
  - `weblogic.server`. Name of the server instance to use for the deployment (for example, `AdminServer` )
  - `weblogic.username`. Administration console username (for example, `weblogic` )
  - `weblogic.password`. Administration console password (for example, `weblogic` )
4. Open a command line window.
5. Change directory to the following, for:
  - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/WebLogic_Sample/build`
  - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/WebLogic_Sample/build`
6. Start the HSQLDB server by entering `ant start.hsqldb`.
7. Compile and deploy the example by entering `ant`.
8. Open a Web Browser.
9. Load the following page: `http://localhost:7001/cspmWeblogicSample`.



## WebLogic Credential Viewer

This example servlet shows you how to use the CSPMClient class to retrieve the credentials.

The CSPMClient class is created using a class factory.

### Class File

```
package com.cloakware.cspm.sample.web;

import java.io.IOException;

import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import com.cloakware.jdbc.StatusCodeMapping;
import com.cloakware.cspm.client.CSPMClient;
import com.cloakware.cspm.sample.ClassFactory;

/**
 * This servlet class is used to retrieve credentials using the
 * CSPMClient class.<br>
 * <br>
 * The user enters a CSPMAlias Name and the servlet displays the information
 * returned by the CSPMClient class. <br>
 * <br>
 * Since the CSPMClient class only returns a status code, the base class
 * provides a class to convert the status code to a more meaningful sentence.
 */
public class CredentialsViewer extends HttpServlet {
    /* Attribute names */
    private final String ERROR_MSG = "errorMsg";

    /* Parameter names and attributes when refreshing the page */
    private final String ALIAS_NAME = "aliasName";
    private final String BYPASS_CACHE = "byPassCache";
    /* Attributes used when displaying credentials/response from
     * the CSPMClient class.
     */
    private final String RETURN_CODE = "returnCode";
    private final String RETURN_MSG = "returnMsg";
    private final String USERNAME = "username";
    private final String PASSWORD = "password";

    /* Error message */
    private final String MSG_ALIAS_EMPTY = "Alias cannot be empty";

    /* Response page */
    private final String TARGET_JSP = "/index.jsp";
    /**
     * Constructor of the object.
     */
}
```

```

public CredentialsViewer() {
    super();
}

/**
 * Destruction of the servlet. <br>
 */
public void destroy() {
    // Just puts "destroy" string in log
    super.destroy();
}

/**
 * The doGet method of the servlet. <br>
 *
 * This method is called when a form has its tag value method equals to get.
 * The method retrieves the alias name and the value of the checkbox
 * indicating if the CSPMClient cache needs to be bypassed. It then calls
 * the retrieveCredentials method of the CSPMClient class and displays the
 * results. <br>
 * <br>
 * An error message is displayed if the alias name is missing.
 *
 * @param request
 *         the request send by the client to the server
 * @param response
 *         the response send by the server to the client
 * @throws ServletException
 *         if an error occurred
 * @throws IOException
 *         if an error occurred
 */
public void doGet(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {

    // Retrieve the parameters
    String alias = (String)request.getParameter(ALIAS_NAME);
    Object byPassCache = request.getParameter(BYPASS_CACHE);
    // Make sure to redisplay the alias name.
    request.setAttribute(ALIAS_NAME, alias);
    request.setAttribute(BYPASS_CACHE,
        (byPassCache != null) ? "checked" : null);

    // if we have an alias
    if (alias != null && !"".equals(alias)) {
        // Class used to retrieve the credential.
        CSPMClient cspmClient = ClassFactory.getCSPMClient();

        // Retrieve the credentials.
        if (byPassCache == null) {
            cspmClient.retrieveCredentials(alias);
        } else {
            cspmClient.retrieveCredentials(alias, "true");
        }
    }
}

```

```

}

// Set the credentials in the request
request.removeAttribute(ERROR_MSG);
request.setAttribute(RETURN_CODE, cspmClient.getStatusCode());
String statusMsg = StatusCodeMapping
.getStatusText(cspmClient);
request.setAttribute(RETURN_MSG, statusMsg);
request.setAttribute(USERNAME, cspmClient.getUserId());
request.setAttribute(PASSWORD, cspmClient.getPassword());
} else {
// return an error message.
request.setAttribute(ERROR_MSG, MSG_ALIAS_EMPTY);
request.removeAttribute(RETURN_CODE);
}

// Get the request dispatcher
RequestDispatcher dispatcher = getServletContext()
.getRequestDispatcher(TARGET_JSP);

// Forward to the jsp file to display the credentials
dispatcher.forward(request, response);
}
}

```

### **WebLogic Connection Pool with HSQLDB Data Store**

This example shows you how to create or modify a data source to use the Credential Manager server for credential retrieval. You can create data source definitions using the WebLogic Server administration console or with Apache ANT scripts. The scripts use the `wlconfig` custom ANT task.

To integrate the A2A Client to your application, change the JDBC driver that is used by the data source. The Credential Manager JDBC driver acts as a proxy JDBC driver serving any JDBC URL that is recognized as a Credential Manager JDBC URL. In the data source configuration, provide information regarding the targeted driver and the alias to use in the special Credential Manager style JDBC URL. The Credential Manager style JDBC URL format is:

```
cspm:[url];CSPMDriver=target.driver;CSPMAlias=alias
```

Form the Credential Manager URL as follows:

- Ensure it begins with the `cspm:` prefix.
- Follow the prefix by the normal JDBC URL, omitting any user/password specification; for example, `jdbc:hsqldb:hsqldb://localhost:9001/cspm1`.
- Set the URL to contain the `CSPMDriver` that indicates an explicit JDBC driver to use.
- Assign, the `CSPMAlias`, which is the alias for the database user in the Credential Manager server, to the URL.

This low-level driver management for connection acquisition means that all new connections obtained for a user whose database password has been changed (by the Credential Manager server) are made using the new password. This action occurs automatically without any knowledge or intervention by any owning data source.

While new connections are obtained using the new password, old connections that were obtained using an old password may linger in the data source pool. Also, if the Credential Manager alias is changed to a new user, then a connection pool has (at least temporarily) a mixture of connections for different actual database users.

Such connection management by the CA Technologies driver ensures that database password changes are transparent to the activities of the data source.

You can configure your data source either with the WebLogic console interface or with the ANT scripts provided with this example.

The ANT scripts that are provided with this example automatically configure the required data sources, so this step is optional.

Execute the following steps in the WebLogic console to create the data source that uses a Credential Manager JDBC driver. Before starting make sure HSQLDB is running. See [HSQL Database Usage](#).

Use the following procedure to configure your data source using the WebLogic console.

**Follow these steps:**

1. From the main window of the console, navigate to **Services > JDBC > Data Sources**.
2. Select **Lock & Edit**.
3. Select **New**.
4. Enter a value for Name; for example, `ExamplesDS`.
5. Enter a value for JNDI Name. Example: `ExamplesDS`
6. For Database Type, select **Other**.
7. Select **Next**.
8. Select the appropriate **Transaction Options**.
9. Select **Next**.
10. For Database Name, enter `cspm1`.
11. For Host Name, enter `localhost`.
12. For Port, enter `9001`.
13. Leave **Database User Name** blank.
14. Leave **Password** and **Confirm Password** blank.
15. Select **Next**.
16. For **Driver Class Name**, enter `com.cloakware.jdbc.JdbcDriver`.
17. For **URL**, enter:  
`cspm:jdbc:hsqldb:hsqldb://localhost:9001/`  
`cspm1;CSPMAlias=hsqldb;CSPMDriver=org.hsqldb.jdbcDriver`
18. Leave **Database User Name** blank.
19. Leave **Password** and **Confirm Password** blank.
20. Leave **Properties** blank.
21. Leave **Test Table Name** blank.
22. Select **Test Connection**. WebLogic should display "Connection test succeeded" at the top of the panel.
23. Select **Next**.
24. Select the target server.
25. Select **Finish**.
26. Select **Activate Changes**.

The following Apache ANT target shows you how to create a connection pool using the Credential Manager JDBC Driver and the data source.

To configure data source using the WebLogic WLConfig Apache Ant task:

```
<!-- Define the wlconfig task -->
<taskdef name="wlconfig" classname="weblogic.ant.taskdefs.management.WLConfig">
<classpath path="${dir.bea.server.lib}/weblogic.jar"/>
</taskdef>
```

```

<!-- Define used to create a DataSource using Cloakware JdbcDriver -->
<target name="datasource.create" depends="">
<wlconfig url="${weblogic.adminurl}"
username="${weblogic.username}"
password="${weblogic.password}">

<query domain="${weblogic.domain}"
type="Server" name="${weblogic.server}"
property="adminserver"/>

<create type="JDBCConnectionPool" name="${datasource.pool.name}"
property="datasource.pool.cspm" >
<set attribute="CapacityIncrement" value="1"/>
<set attribute="DriverName" value="com.cloakware.jdbc.JdbcDriver"/>
<set attribute="InitialCapacity" value="5"/>
<set attribute="MaxCapacity" value="10"/>
<set attribute="RefreshMinutes" value="0"/>
<set attribute="ShrinkPeriodMinutes" value="1"/>
<set attribute="ShrinkFrequencySeconds" value="30"/>
<set attribute="ShrinkingEnabled" value="true"/>
<set attribute="TestConnectionsOnRelease" value="false"/>
<set attribute="TestConnectionsOnReserve" value="true"/>
<set attribute="URL" value="cspm:jdbc:hsqldb:hsqldb://localhost:9001/cspm1;
CSPMAlias=hsqldb;
CSPMDriver=org.hsqldb.jdbcDriver"/>
<set attribute="Targets" value="${adminserver}"/>
<set attribute="TestTableName" value="PUBLIC.TESTTBL"/>
</create>

<create type="JDBCDataSource"
name="${datasource.ds.name}"
property="datasource.cspm">
<set attribute="JNDIName" value="CSPM${datasource.jndi.name}"/>
<set attribute="PoolName" value="CSPM${datasource.pool.name}"/>
<set attribute="Targets" value="${adminserver}"/>
</create>
</wlconfig>
</target>

```

### **Register WebLogic Requestor**

See [Add and Run Credential Manager A2A Requestors](#) for the procedure to register your requestor with Credential Manager. Use the following data.

Parameter	Description
Script Name	com.cloakware.cspm.sample.web.CredentialsViewer
Execution Path	C:\bea\user_projects\domains\cloakware

Type	Java
------	------

Parameter	Description
Script Name	com.cloakware.client.jdbc.JdbcDriver
Execution Path	C:\bea\user_projects\domains\cloakware
Type	Java

HSQldb is an SQL relational database engine that is written in Java. It is used in the example as the database server. See also:

- [Register HSQldb as a Target Application](#)
- [Register Mapping between Request Server and Target Alias](#)
- [HSQL Database Usage](#)

## Integrate a Java Application with the A2A Client on WebSphere CE

This example uses the A2A Client to manage the credentials that are used by a Java container JDBC connection pool within WebSphere Application Server Community Edition (WebSphere CE).

This example uses a credential viewer and an HSQldb data store to show the following information:

- The credential viewer shows you how to view credentials that are stored in the Credential Manager server using the `CSPMClient` Java class. Use this example for simple integration and to test the ability to connect to Credential Manager and retrieve credentials. The example displays the credentials to the screen.
- The HSQldb data store shows you how to configure a data store using the `CredentialManagerJdbcDriver` Java class to retrieve credentials and connect to an HSQldb data store. The example retrieves credentials and uses them to access a data store.

### NOTE

For historical reasons, A2A is referred to as CSPM in code samples, file, and environment variable names.

This example is available on all A2A Client installations in the following directories:

- **UNIX:** `$CSPM_CLIENT_HOME/cloakware/cspmclient/examples/java/WebSphere_Sample`
- **Windows:** `%CSPM_CLIENT_HOME%/cloakware/cspmclient/examples/java/WebSphere_Sample`

File	Description
<code>ClassFactory.java</code>	Class factory that is used to create the objects that are used in the example web application. The class allows you to create the <code>CSPMClient</code> class and to perform a lookup in the Initial Context to retrieve the data source that is used to get a connection to the database.
<code>CredentialsViewer.java</code>	Servlet class that is used to connect to the Credential Manager server to retrieve credentials.
<code>ConnectionTester.java</code>	Servlet class that is used to create 10 connections to a database and execute a basic SQL statement. The class retrieves the <code>DataSource</code> class using the <code>ClassFactory</code> class.

## Integration Process for WebSphere CE

Use the following process to modify your application to use the Credential Manager server to manage credentials:

1. Configure development environment. See [Configure your Development Environment for WebSphere CE](#).

2. Optionally, integrate the A2A Client to retrieve credentials. See [WebSphere CE Credential Viewer](#).
3. Create or modify the data source file. See [WebSphere CE Connection Pool with HSQLDB Data Store](#).
4. Register requestor. See [Register WebSphere CE Requestor](#).

### **Configure your Development Environment for WebSphere CE**

You must configure your development environment for both WebSphere CE development and Credential Manager integration.

The example contains an Apache ANT build file that is located in the build directory that you can use to create the WAR file and to deploy it. The build file is compatible with ANT 1.6.5 and above.

#### **Configure Your Environment for WebSphere CE Development**

Use the following procedure to configure your environment for WebSphere CE development.

##### **Follow these steps:**

1. Install WebSphere Application Server Community Edition 2.0. See <http://www.ibm.com/developerworks/downloads/ws/wasce/>.
2. Install Apache ANT 1.6.5 or above. See <http://ant.apache.org/bindownload.cgi>.
3. Set the `ANT_HOME` environment variable. See <http://ant.apache.org/manual/install.html>.
4. Install the Java Database HSQLDB 1.8.0. See [http://sourceforge.net/project/showfiles.php?group\\_id=23316](http://sourceforge.net/project/showfiles.php?group_id=23316).
5. Set the `HSQL_HOME` environment variable to the path where you installed HSQL (for example, `opt/tools/hsqldb`).

#### **Configure Your Environment for A2A Client Integration with WebSphere CE**

Use the following procedure to configure your environment for A2A Client integration with WebSphere CE.

##### **Follow these steps:**

1. [Install the A2A Client](#).
2. Create or add to the `JAVA_OPTS` environment variable:
  - UNIX:
    - Djava.library.path=\$CSPM\_CLIENT\_HOME\lib
    - Dcspm\_client\_config\_file=\$CSPM\_CLIENT\_HOME\config\cspm\_client\_config.xml
  - Windows:
    - Djava.library.path=%CSPM\_CLIENT\_HOME%\lib
    - Dcspm\_client\_config\_file=%CSPM\_CLIENT\_HOME%\config\cspm\_client\_config.xml
3. Edit the `$WEBSPPHERE_HOME/var/config/config.xml` file. Locate the `<gbean name="TomcatAJPConnector">` XML element and modify the port attribute below it as follows:
 

From:

```
<gbean name="TomcatAJPConnector">
<attribute name="host">${ServerHostname}</attribute>
<attribute name="port">${AJPPrimary}</attribute>
```

To:

```
<gbean name="TomcatAJPConnector">
<attribute name="host">${ServerHostname}</attribute>
<attribute name="port">8010</attribute>
```
4. Register the `cspmclient.jar` file with WebSphere CE as an artifact. To do so, log in to the Administration Console and select Common Libs as follows:
  - a. Select Browse to locate the `cspmclient.jar` in the following locations:
    - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/lib`
    - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/lib`
  - b. Enter `cspmclient` for Group.
  - c. Enter `cspmclient` for Artifact.

- d. Enter 3.5 for Version.
  - e. Enter `jar` for Type.
  - f. Select **Install** to add the JAR file to the repository.
5. Register the `cloakwareJdbc.jar` file with WebSphere CE as an artifact. To do so, log in to the Administration Console and select Common Libs as follows:
- a. Select Browse to locate the `cloakwareJdbc.jar` in the following locations:
    - UNIX: `$CSPM_CLIENT_HOME/cloakware/cspmclient/tools`
    - Windows: `%CSPM_CLIENT_HOME%/cloakware/cspmclient/tools`
  - b. Enter `cloakwareJdbc` for Group.
  - c. Enter `cloakwareJdbc` for Artifact.
  - d. Enter 3.5 for Version.
  - e. Enter `jar` for Type.
  - f. Select **Install** to add the JAR file to the repository.

### **Configure Your Environment for HSQLDB**

Use the following process to configure your environment for HSQLDB.

#### **Follow these steps:**

1. Register the `hsqldb.jar` file with WebSphere CE as an artifact. To do so, log in to the Administration Console and select Common Libs as follows:
  - a. Select Browse to locate the `hsqldb.jar` in the following locations:
    - UNIX: `$HSQL_HOME/lib`
    - Windows: `%HSQL_HOME%/lib`
  - b. Enter `hsqldb` for Group.
  - c. Enter `hsqldb` for Artifact.
  - d. Enter 1.8.0.2 for Version.
  - e. Enter `jar` for Type.
  - f. Select **Install** to add the JAR file to the repository.

### **Configure Your Database Pool Using the WebSphere CE Administration Console**

Use the following procedure to configure your database pool using the WebSphere CE Administration Console.

#### **Follow these steps:**

1. Verify that HSQLDB is running. See [HSQL Database Usage](#).
2. From the main window of the console, navigate to the Database Pools display.
3. Select "Using the Geronimo database pool wizard" to create a database pool.
4. Enter a value for Name of Database Pool. For the example web application, you must enter `CSPMSampleDS`.
5. Select `Other` for Database Type.
6. Select **Next**.
7. For JDBC Driver Class, enter `com.cloakware.jdbc.JdbcDriver`.
8. For Driver JAR, press the **Ctrl** key and select all the following entries:
  - `cspmclient/cspmclient/3.5/jar`
  - `cloakwareJdbc/cloakwareJdbc/3.5/jar`
  - `hsqldb/hsqldb/1.8.0.2/jar`
9. Leave DB User Name blank.
10. Leave DB Password and Confirm Password blank.
11. Select **Next**.
12. For JDBC Connect URL, enter:
 

```
cspm:jdbc:hsqldb:hsqldb://localhost:9001/cspm1;CSPMAlias=hsqldb;CSPMDriver=org.hsqldb.jdbcDriver
```



13. Leave the Connection Pool Parameters blank.
14. Select **Test Connection**. WebSphere CE displays “Connected to HSQL Database Engine 1.8.0” at the top of the panel.
15. Select **Deploy**.

### **Create a Second Database Pool**

To run the sample WebSphere CE application, create a second database pool as follows:

#### **Follow these steps:**

1. From the main window of the console, navigate to the Database Pools display.
2. Select “Using the Geronimo database pool wizard” to create a database pool.
3. Enter `SampleDS` as the value for Name of Database Pool.
4. Select `Other` for Database Type.
5. Select **Next**.
6. Enter `org.hsqldb.jdbcDriver` for JDBC Driver Class.
7. Select `hsqldb/hsqldb/1.8.0.2/jar` for Driver JAR.
8. Enter `TestUser` for DB User Name.
9. Enter `Test` for DB Password and Confirm Password.
10. Select **Next**.
11. Enter `jdbc:hsqldb:hsq1://localhost:9001/cspm1` for JDBC Connect URL.
12. Leave the Connection Pool Parameters blank.
13. Select **Test Connection**. WebSphere CE displays “Connected to HSQL Database Engine 1.8.0” at the top of the panel.
14. Select **Deploy**.

### **Deploy and Run the Sample WebSphere CE Application**

Use the following procedure to compile and run the sample web application using an Apache ANT task.

#### **Follow these steps:**

1. Ensure WebSphere CE is running and you have completed the following steps:
  - The steps to configure your environment for A2A Client integration with WebSphere CE, described in [Configure your Development Environment for WebSphere CE](#)
  - The steps to configure your environment for HSQLDB, described in [Configure your Development Environment for WebSphere CE](#)
  - The steps to configure your database pool using the WebSphere CE Administration Console, described in [WebSphere CE Connection Pool with HSQLDB Data Store](#)
  - The steps to run the sample WebSphere CE application, described in [WebSphere CE Connection Pool with HSQLDB Data Store](#)
2. With a text editor (such as NotePad or Vim), edit the `build.properties` file located in the following directories:
  - UNIX: `$CSPM_CLIENT_HOME/cspmclient/examples/java/WebSphere_Sample/build`
  - Windows: `%CSPM_CLIENT_HOME%/cspmclient/examples/java/WebSphere_Sample/build`
3. Change the value of the `dir.server` property (for example, to `C:/Program Files/IBM/WebSphere/AppServerCommunityEdition`) and save the file.
4. Open a command line window.
5. Change directory to the following location:
  - UNIX: `$CSPM_CLIENT_HOME/cspmclient/examples/java/WebSphere_Sample/build`
  - Windows: `%CSPM_CLIENT_HOME%/cspmclient/examples/java/WebSphere_Sample/build`
6. Start the HSQLDB server by entering `ant start.hsqldb`.

7. Compile and deploy the example by entering `ant`.
8. Open a Web Browser.
9. Load the following page: <https://localhost:8443/cspmWebsphereSample>

### **WebSphere CE Credential Viewer**

This example servlet shows you how to use the `CSPMClient` class to retrieve the credentials.

The `CSPMClient` class is created using a class factory.

#### ***Class File***

```
package com.cloakware.cspm.sample.web;

import java.io.IOException;

import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import com.cloakware.jdbc.StatusCodeMapping;
import com.cloakware.cspm.client.CSPMClient;
import com.cloakware.cspm.sample.ClassFactory;

/**
 * This servlet class is used to retrieve credentials using the
 * CSPMClient class.<br>
 * <br>
 * The user enters a CSPMAlias Name and the servlet displays the information
 * returned by the CSPMClient class. <br>
 * <br>
 * Since the CSPMClient class only returns a status code, the base class
 * provides a class to convert the status code to a more meaningful sentence.
 */
public class CredentialsViewer extends HttpServlet {
    /* Attribute names */
    private final String ERROR_MSG = "errorMsg";

    /* Parameter names and attributes when refreshing the page */
    private final String ALIAS_NAME = "aliasName";
    private final String BYPASS_CACHE = "byPassCache";
    /* Attributes used when displaying credentials/response from
     * the CSPMClient class.
     */
    private final String RETURN_CODE = "returnCode";
    private final String RETURN_MSG = "returnMsg";
    private final String USERNAME = "username";
    private final String PASSWORD = "password";

    /* Error message */
    private final String MSG_ALIAS_EMPTY = "Alias cannot be empty";
```

---

```

/* Response page */
private final String TARGET_JSP = "/index.jsp";
/**
 * Constructor of the object.
 */
public CredentialsViewer() {
    super();
}

/**
 * Destruction of the servlet. <br>
 */
public void destroy() {
    // Just puts "destroy" string in log
    super.destroy();
}

/**
 * The doGet method of the servlet. <br>
 *
 * This method is called when a form has its tag value method equals to get.
 * The method retrieves the alias name and the value of the checkbox
 * indicating if the CSPMClient cache needs to be bypassed. It then calls
 * the retrieveCredentials method of the CSPMClient class and displays the
 * results. <br>
 * <br>
 * An error message is displayed if the alias name is missing.
 *
 * @param request
 *         the request send by the client to the server
 * @param response
 *         the response send by the server to the client
 * @throws ServletException
 *         if an error occurred
 * @throws IOException
 *         if an error occurred
 */
public void doGet(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {

    // Retrieve the parameters
    String alias = (String)request.getParameter(ALIAS_NAME);
    Object byPassCache = request.getParameter(BYPASS_CACHE);
    // Make sure to redisplay the alias name.
    request.setAttribute(ALIAS_NAME, alias);
    request.setAttribute(BYPASS_CACHE,
        (byPassCache != null) ? "checked" : null);

    // if we have an alias
    if (alias != null && !"".equals(alias)) {
        // Class used to retrieve the credential.
        CSPMClient cspmClient = ClassFactory.getCSPMClient();

```

```

// Retrieve the credentials.
if (byPassCache == null) {
    cspmClient.retrieveCredentials(alias);
} else {
    cspmClient.retrieveCredentials(alias, "true");
}

// Set the credentials in the request
request.removeAttribute(ERROR_MSG);
request.setAttribute(RETURN_CODE, cspmClient.getStatusCode());
String statusMsg = StatusCodeMapping
    .getStatusText(cspmClient);
request.setAttribute(RETURN_MSG, statusMsg);
request.setAttribute(USERNAME, cspmClient.getUserId());
request.setAttribute(PASSWORD, cspmClient.getPassword());
} else {
    // return an error message.
    request.setAttribute(ERROR_MSG, MSG_ALIAS_EMPTY);
    request.removeAttribute(RETURN_CODE);
}

// Get the request dispatcher
RequestDispatcher dispatcher = getServletContext()
    .getRequestDispatcher(TARGET_JSP);

// Forward to the jsp file to display the credentials
dispatcher.forward(request, response);
}
}

```

### **WebSphere CE Connection Pool with HSQLDB Data Store**

This example shows you how to create or modify a data source to use the Credential Manager server for credential retrieval. The data source definitions are created with the WebSphere CE Administration Console.

To integrate the A2A Client to your application, change the JDBC driver that is used by the data source. The Credential Manager JDBC driver acts as a proxy JDBC driver serving any JDBC URL that is recognized as a Credential Manager JDBC URL. In the data source configuration, provide information regarding the targeted driver and the alias to use in the special Credential Manager style JDBC URL. The Credential Manager style JDBC URL format is:

```
cspm:[url];CSPMDriver=target.driver;CSPMAlias=alias
```

Form the Credential Manager URL as follows:

- Ensure it begins with the `cspm:` prefix.
- Follow the prefix by the normal JDBC URL, omitting any user/password specification; for example, `jdbc:hsqldb:hsqldb://localhost:9001/cspm1`.
- Set the URL to contain the `CSPMDriver` that indicates an explicit JDBC driver to use.
- Assign the `CSPMAlias`, which is the alias for the database user in the Credential Manager server, to the URL.

This low-level driver management for connection acquisition means that all new connections that are obtained for a user whose database password has been changed (by the Credential Manager server) are made using the new password. This action occurs automatically without any knowledge or intervention by any owning database pool.

While new connections are obtained using the new password, old connections that were obtained using an old password may linger in the database pool. Also, if the Credential Manager alias is changed to a new user, then a connection pool has (at least temporarily) a mixture of connections for different actual database users.

Such connection management by the CA Technologies driver ensures that database password changes are transparent to the database pool activities.

### Register WebSphere CE Requestor

See [Add and Run Credential Manager A2A Requestors](#) for the procedure to register your requestor with Credential Manager. Use the following data.

Parameter	Description
Script Name	com.cloakware.cspm.sample.web.CredentialsViewer
Execution Path	C:\Program Files (x86)\IBM\WebSphere\AppServerCommunityEdition\bin
Type	Java

Parameter	Description
Script Name	com.cloakware.client.jdbc.JdbcDriver
Execution Path	C:\Program Files (x86)\IBM\WebSphere\AppServerCommunityEdition\bin
Type	Java

HSQldb is an SQL relational database engine that is written in Java. HSQldb is used in the example as the database server. See also:

- [Register HSQldb as a Target Application](#)
- [Register Mapping between Request Server and Target Alias](#)
- [HSQldb Database Usage](#)

## Integrate Apps to Use the Credential Manager A2A Client on UNIX and AIX

This section includes examples of UNIX and AIX applications that have been integrated to use Credential Manager to retrieve target account credentials using the A2A Client.

Use the table of contents to access the topics in this section.

### Integrate a Perl Script with A2A Client on UNIX or AIX

This example uses the `example.pl` script in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory. It uses a UNIX executable to integrate the A2A Client (`cspmclient`) with UNIX or AIX.

#### Code: Perl Script with A2A Client on UNIX or AIX

```
#!/usr/bin/perl -w

use strict;
use lib "/opt/catech/cspmclient/lib";
use CSPM_CLIENT;
```

```

my ($alias, $answer, $bypass_cache, $command, $password, $src, $userid, $msg, @a
ray,$isXMLOutput, $argv);

$msg="";
$bypass_cache = "";
$alias = "";
$isXMLOutput = 0;

foreach $argv (@ARGV){
    if($argv eq "-x"){
        $isXMLOutput = 1;
    }
}
# $GETCR = "GET CRedentials" ; defined in the CSPM_CLIENT.pm
# it is the main and only call when using Perl to retrieve
# the userid and password from the Password Authority Server

$command = qq{$GETCR @ARGV};
$answer = ` $command `;

if($isXMLOutput){
    print qq($answer\n);
}else{
    @array = split(/\s+/, $answer);
    print qq(Return Code: $array[0]\n);
    print qq(UserID:      $array[1]\n);
    print qq>Password:    $array[2]\n);

    if ($array[0] ne "400" ) {
        for my $i (3..$#array){
            $msg = $msg." ".$array[$i];
        }
        print qq(Message: $msg\n);
    } else {
        print qq(PASSED\n);
    }
}

# End of Main

__END__

```

### **Register Requestor - Perl Script with A2A Client on UNIX or AIX**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, `example.pl`.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `Perl`.

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate a C or C++ Application with A2A Client on UNIX or AIX

This example uses the `example.c` script in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory. It uses a UNIX executable to integrate the A2A Client (`cspmclient`) with UNIX or AIX.

The path to the binary client depends on `CSPM_CLIENT_HOME` being set. For the A2A Client, the path is `$CSPM_CLIENT_HOME/cspmclient/bin/cspmclient`.

The A2A Client (`cspmclient`) accepts up to two command line arguments. This example accepts and passes those arguments from the command line:

- `argv[1]`. Provides the target alias name. This argument is mandatory.
- `argv[2]`. Provides the Bypass Cache Flag, which can be `true` or `false`. The default is `false`. This argument is optional.

The `example.c` script has been compiled to produce the `example_c_interface_java` executable also located in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory.

### Code: C Application with A2A Client on UNIX

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define CSPM_CLIENT_BINARY "/cspmclient/bin/cspmclient"
#define BUF_SIZE 256

int main (int argc, char **argv)
{
    FILE *results_file;

    /* Declarations, Allocations & Initializations */

    int error = 0;

    char *cspm_client_home, *return_code, *userid, *password;

    char a_buffer[BUF_SIZE];
    char command[BUF_SIZE];
    char bypass_cache_flag[BUF_SIZE];

    memset(a_buffer, '\0', BUF_SIZE);
    memset(command, '\0', BUF_SIZE);
    memset(bypass_cache_flag, '\0', BUF_SIZE);

    /* Validate Command Line Arguments */

    if ( argv[1] == NULL ) {
        printf("\nERROR: arg[1] cannot be NULL\n\n");
        exit(1);
    }

    if ( argv[2] == NULL ) {
```

```
    printf("\nNo Bypass Cache Flag provided - will use the default\n");
    sprintf(bypass_cache_flag, "%s", "false");
} else {
    sprintf(bypass_cache_flag, "%s", argv[2]);
}

/* Get the CSPM_CLIENT_HOME */

cspm_client_home=getenv("CSPM_CLIENT_HOME");

if ( cspm_client_home == NULL ) {
    printf("\nGlobal Environment Variable CSPM_CLIENT_HOME is not set\n");
    exit(1);
}

/*
Command Line Creation
NOTE: No space in the format string for the first 2 list elements - %s%s
*/

sprintf (
    command,
    "%s%s %s %s",
    cspm_client_home,
    CSPM_CLIENT_BINARY,
    argv[1],
    bypass_cache_flag
);

/* We will be using a popen call to execute but also to retrieve
the standard output returned by the client execution */

results_file = popen(command, "r");

while ( fgets(a_buffer,BUF_SIZE,results_file) != NULL ) {

    /* Parse the output to retrieve the fields we are interested in */

    if( (return_code = (char *) strtok(a_buffer," ")) != NULL ) {
        if ( (userid = (char *) strtok(NULL," ")) != NULL ) {
            if ( (password = (char *) strtok(NULL," ")) == NULL )
                error = 1;
        }
        else
            error = 1;
    }
    else
        error = 1;
}

pclose(results_file);

/* Print results */
```



```

if ( error ) {
    printf("\nFailed to retrieve the credentials\n");
    exit(99);
} else {
    printf("\nreturn_code:\t%s\n",return_code);
    printf("userid:\t\t%s\n",userid);
    printf("password:\t%s\n",password);
}
}

```

### **Register Requestor - C or C++ Application with A2A Client on UNIX or AIX**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension. For example, example.c.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type. For example, C or C++.

When entering the file and execution paths, you must specify the absolute paths without links.

### **Integrate a Korn Shell Script with A2A Client on UNIX or AIX**

This example uses the `example.ksh` script in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory. It uses a UNIX executable to integrate the A2A Client (`cspmclient`) with UNIX or AIX.

The example applies to the Korn shell (`#!/bin/ksh`).

The path to the binary client depends on `CSPM_CLIENT_HOME` being set.

The A2A Client (`cspmclient`) accepts up to two command line arguments. This example accepts and passes these arguments from the command line:

- \$1. Provides the target alias name. This argument is mandatory.
- \$2. Provides the Bypass Cache Flag, which can be `true` or `false`. The default is `false`. This argument is optional.

### **Code: Korn shell script with A2A Client on UNIX or AIX**

```

#!/bin/ksh
CSPM_CLIENT_BINARY="/cspmclient/bin/cspmclient"

# Validate Required Arguments

if [ ! CSPM_CLIENT_HOME ]
then
    echo "Global Environment Variable CSPM_CLIENT_HOME is not set"
    echo "Aborting..."
    exit 1
fi

if [ ! $1 ]
then
    echo "No Target Alias provided "

```

```

    echo "Aborting..."
    exit 2
else
    target_alias="$1"
fi

if [ ! $2 ]
then
    bypass_cache="false"
else
    bypass_cache="$2"
fi

# Action

command="$CSPM_CLIENT_HOME$CSPM_CLIENT_BINARY $target_alias $bypass_cache"

result=`$command`

return_code=`echo $result | awk '{print($1)}'`
userid=`echo $result | awk '{print($2)}'`
password=`echo $result | awk '{print($3)}'`

echo "Return Code: $return_code"
echo "User ID:      $userid"
echo "Password:     $password"

```

### **Register Requestor - Adding a Korn shell script with A2A Client on UNIX or AIX**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, `example.ksh`.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `Korn shell` script.

When entering the file and execution paths, you must specify the absolute paths without links.

### **Integrate a C Shell Script with A2A Client on UNIX or AIX**

This example uses the `example.csh` script in the `$CSPM_CLIENT_HOME/cspmclient/examples` directory. It uses a UNIX executable to integrate the A2A Client (`cspmclient`) with UNIX or AIX.

The path to the binary client depends on `CSPM_CLIENT_HOME` being set.

The A2A Client (`cspmclient`) accepts up to two command line arguments. This example accepts and passes these two arguments from the command line:

- \$1. This argument provides the target alias name. This argument is mandatory.
- \$2. This argument provides the Bypass Cache Flag, which can be `true` or `false`. The default is `false`. This argument is optional.

**Code: C Shell Script with A2A Client on UNIX or AIX**

```
#!/bin/csh
set CSPM_CLIENT_BINARY="/cspmclient/bin/cspmclient"

# Validate Required Arguments

if ( $CSPM_CLIENT_HOME == "" ) then
    echo "Global Environment Variable CSPM_CLIENT_HOME is not set"
    echo "Aborting..."
    exit 1
endif

if ( $1 == "" ) then
    echo "No Target Alias provided "
    echo "Aborting..."
    exit 2
else
    set target_alias="$1"
endif

if ( $2 == "" ) then
    set bypass_cache="false"
else
    set bypass_cache="$2"
endif

# Action

set command="$CSPM_CLIENT_HOME$CSPM_CLIENT_BINARY $target_alias $bypass_cache"

set result=`$command`

set return_code=`echo $result | awk '{print($1)}'`
set    userid=`echo $result | awk '{print($2)}'`
set    password=`echo $result | awk '{print($3)}'`

echo "Return Code: $return_code"
echo "User ID:      $userid"
echo "Password:     $password"
```

**Register Requestor - C shell Script with A2A Client on UNIX or AIX**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, `example.csh`.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `C shell script`.

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate a PHP Script with A2A Client on UNIX

The following PHP script uses a UNIX executable to integrate the A2A Client (`cspmcclient`). Your installed A2A Client does not contain a soft copy of this script.

### IMPORTANT

PHP is *not* supported for use with AIX.

### Code: PHP Script with A2A Client on UNIX

```
<?php

#####
#
# Php example. To execute, do:
# prompt> php test2.php
#
#####

$alias="test";
$bypassCacheFlag="false";

$data = getCredential($alias,$bypassCacheFlag);
echo "Return code: $data[retCode]\n";
echo "User name: $data[user]\n";
echo "Password: $data[password]\n";

function getCredential($inAlias,$inFlag){

    $exec    = "/opt/cloakware/cspmcclient/bin/cspmcclient";
    $command = "$exec $inAlias $inFlag";
    $hndl=popen($command,'r') or die ("Unable to open pipe for command $command\n");

    echo "About to execute command: $command\n";
    $retVal=fread($hndl,2096) or die ("Unable to execute command $command\n");
    $n = sscanf($retVal, "%s %s %s", $retCode, $user, $password);
    $arr=array("retCode" => $retCode,
        "user"          => $user,
        "password"      => $password);
    return $arr;
}
?>
```

### Register Requestor - PHP Script with A2A Client on UNIX

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, the name of the PHP script example given in [Code: PHP Script with A2A Client on UNIX](#).
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `PHP`.

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate a Python Script with A2A Client on UNIX and AIX

The following Python script uses a UNIX executable to integrate the A2A Client (`cspmclient`) with UNIX or AIX. Your installed A2A Client does not contain a soft copy of this script.

### **Code: Python Script with A2A Client on UNIX or AIX**

```
#!/usr/bin/env python

import commands
import os,time
import sys

def getCredential(alias, cacheflag, optflag):
    cmd = "/opt/cloakware/cspmclient/bin/cspmclient" + " " + alias+ " "+cacheflag+" "+optflag
    # print cmd
    f=os.popen(cmd)
    retVal= f.read()
    print retVal

if __name__ == "__main__":
    alias=""
    cacheflag=""
    optflag=""

    argc = len(sys.argv)
    if argc > 1:
alias=sys.argv[1]
        if (argc == 3) and (argc != "-x"):
            cacheflag = sys.argv[2]
        elif (argc == 3) and (argc == "-x"):
            optflag = sys.argv[2]
        elif (argc == 4):
            optflag = sys.argv[3]
        else:
dummy=1
            getCredential(alias, cacheflag, optflag)
```

### **Register Requestor - Python Script with A2A Client on UNIX or AIX**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension. For example, the name of the Python script example given in the previous example.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `Other`.

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate Apps to Use the Credential Manager A2A Client on Windows

The content in this section provides examples of Windows applications that have been integrated to use Credential Manager to retrieve target account credentials using the A2A Client.

If you are using A2A Clients and the data returned (accounts and passwords) is limited to ANSI characters, no character set conversion is required. The client returns ANSI characters as single-byte UTF-8 characters. However, if you are using A2A Clients and the data returned includes non-ANSI UTF-8 characters, a character conversion may be required. Contact CA Support for assistance, and reference UTF-16 conversion.

Use the table of contents to access the topics in this section.

### Integrate a Perl Script with A2A Client on Windows

The following Perl script uses a Windows Perl Module (CSPM\_CLIENT\_WIN.pm) to integrate the A2A Client (cspmclient.exe). Your installed A2A Client contains CSPM\_CLIENT\_WIN.pm but does not contain a soft copy of the following script.

#### Code: Perl Script with A2A Client on Windows

```
#!/c:/perl/bin/perl -w
#Example to show how to get account info by using perl in windows.
#Need to: 1) Include a module, CSPM_CLIENT_WIN.pm.
# 2) Use the $EXEC string from the module.
# 3) Add Target server alias.

use strict;
use warnings;
use lib "c:/cspm/catech/cspmclient/lib";
use CSPM_CLIENT_WIN;

my $exec=$EXEC . "targetAlias" ;
my $param=`$exec`;
my @param2 = split(/\s+/, $param);
my $errorCode=$param2[0];
if($errorCode eq '400')
{
    my $userID=$param2[1];
    my $passWd=$param2[2];
    print "userId = " . $userID . "\n";
    print "password = " . $passWd . "\n";
}
else
{
    print "Failed to retrieve credentials... errorcode=" . $errorCode;
}
```

#### Register Requestor - Perl Script with A2A Client on Windows

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, the name of the Perl script example given in [Code: Perl Script with A2A Client on Windows](#).
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, Perl .

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate a Visual Basic Application

This example uses a Visual Basic project (Project1.vbp ) and the VB\_Sample.exe executable in the \$CSPM\_CLIENT\_HOME\cloakware\cspmclient\examples\VB\_Sample directory. It uses the CA Technologies MFC DLL (cspmclientc.dll ) to integrate the A2A Client.

### Code: Visual Basic Application

```
' From within your VB project:
'   Select Project
'   Projects
' From the References window, select Browse.
' Navigate to c:\cspm\cloakware\cspmclient\lib\
' Select the cspmclientc.dll file.
'
' Your project will now have a reference to the cspmclientc.dll.
'
' Next you need to uncommment the line - 'Dim X As New ccspmclientc' from the Command1_Click() method
'
```

```
Private Sub Command1_Click()

    '*** Uncomment the following line
    'Dim X As New ccspmclientc

    Dim ret As Long
    Dim userId As String
    Dim password As String
    Dim targetAlias As String
    Dim options As String
    Dim xml As String
    Dim bypassCache As String
    Dim xmlOutput As Boolean
    xmlOutput = False

    bypassCache = "false"

    targetAlias = Me.targetAliasName

    If (Me.bypassCacheCheck.Value = vbChecked) Then
        bypassCache = "true"
        options = options + "-b"
    End If
```

```

If (Me.xmlOutputCheck.Value = vbChecked) Then
    options = options + " -x"
    xmlOutput = True
End If

'Uncomment the line - 'Dim X As New ccspmlclientc' - at the begining of this method if you get an error on
this line.
ret = X.retrieveCredentials(targetAlias, bypassCache, options)

If (xmlOutput) Then
    Me.results = X.getXMLData
Else
    If (ret = 400) Then

        userId = X.getUserId()
        password = X.getPassword()
        xml = X.getXMLData

        MsgBox "userId = " + userId + ", password=" + password + Chr$(13) + xml, vbOKOnly, Me.Caption

    Else
        MsgBox "Failed to process request with errorCode: " + CStr(ret), vbOKOnly, Me.Caption
    End If
End If
End Sub

```

### **Register Requestor - Visual Basic Application**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, `VB_Sample.exe`.
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, `Visual Basic`.

When entering the file and execution paths, you must specify the absolute paths without links.

### **Integrate a Visual C++ Application**

This example uses the `VC_Sample.dsp` project file and the `VC_Sample.cpp` file in the `$CSPM_CLIENT_HOME\cloakware\ccspmlclient\examples\VC_Sample` directory. It uses the CA Technologies MFC DLL to integrate the A2A Client.

#### **Code: Visual C++ Application**

```

// VC_Sample.cpp : Defines the entry point for the console application.
//
#include "stdafx.h"
#include <afxwin.h>
#include <atlbase.h>
#include "stdafx.h"

```



```

#import "c:\cspm\cloakware\cspmclient\lib\cspmclientc.tlb"

#define ERROR_CODE_SUCCESS400
#define ERROR_CODE_BADPARAM407

int main(int argc, char* argv[])
{
    USES_CONVERSION;
    _bstr_t targetAlias = _bstr_t("sample");
    _bstr_t bypassFlg = _bstr_t("false");
    _bstr_t bstrUserId, bstrPassword, bstrXMLData, bstrMessage;
    _bstr_t cliOpt = _bstr_t("");
    char* userId;
    char* password;
    char* xmlData;
    char* message;
    char *szTmp;
    BOOL isXMLOutput = FALSE;
    HRESULT hr;
    CLSID cls;

    using namespace Cspmclientc;

    if(argc>1)
    {
        targetAlias = _bstr_t(argv[1]);
        for (int pos = 2; pos < argc; pos++){
            if(pos == 2 && argv[pos][0] != '-'){
                bypassFlg = _bstr_t(argv[pos]);
            }else{
                if(!strcmp(argv[pos], "-x"))
                    isXMLOutput = TRUE;
                cliOpt = cliOpt+ " "+_bstr_t(argv[pos]);
            }
        }
        // Intializing the com component
        CoInitialize(NULL);
        hr = CLSIDFromProgID(OLESTR("cspmclientc.ccspmclientc"), &cls);
        Iccspmclientc *t;
        hr = CoCreateInstance(cls, NULL, CLSCTX_INPROC_SERVER, __uuidof(Iccspmclientc), (LPVOID *) &t);

        //printf("Retrieving credentials for %s\n", (char* )targetAlias);
        int retVal = -1;
        retVal = t->retrieveCredentials(targetAlias, bypassFlg, cliOpt); //call method
        if(isXMLOutput){
            bstrXMLData = t->getXMLData();
            xmlData = OLE2T(bstrXMLData);
            SysFreeString(bstrXMLData);
            printf("Block data: %s\n", xmlData);
        }
    }
}

```

```

}else if(retval==ERROR_CODE_SUCCESS){

    bstrUserId = t->getUserId();
    bstrPassword = t->getPassword();

    userId= OLE2T(bstrUserId);
    password= OLE2T(bstrPassword);

    printf("ErrorCode: %i\n",retval);
    printf("UserID: %s\n", userId);
    printf("Password: %s\n", password);

    SysFreeString(bstrUserId);
    SysFreeString(bstrPassword);

}else{

    bstrMessage = t->getMessage();
    message = OLE2T(bstrMessage);
    printf("ErrorCode: %i\n",retval);
    printf("UserID: %s\n", "null");
    printf("Password: %s\n", "null");
    printf("Message: %s\n", message);
    SysFreeString(bstrMessage);
}

t->Release();

CoUninitialize();
}else{
printf("ErrorCode: %i\n",ERROR_CODE_BADPARAM);
    printf("UserID: %s\n", "null");
    printf("Password: %s\n", "null");
    }
return 0;
}

```

### **Register Requestor - Visual C++ Application**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, VC\_Sample.cpp .
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, Visual C++ .

When entering the file and execution paths, you must specify the absolute paths without links.

## Integrate a C#.NET Application using IIS Application Server

This example uses the A2A Client to manage the credentials used by a C#.NET connection class within an Internet Information Service (IIS) application server. The example uses a Windows DLL (`cspmclientc.dll`) to integrate the A2A Client.

This example uses a credential viewer and an SQL Server 2005 Express Edition data store to show the following:

- The credential viewer shows you how to view credentials stored in the Credential Manager server using the `CSPMClient` COM component. Use this example for simple integration and to test the ability to connect to Credential Manager and retrieve credentials. The example displays the credentials to the screen.
- The SQL Server 2005 Express Edition data store shows you how to configure a connection string used by the `Connection` class to retrieve credentials and connect to an SQL Server 2005 Express Edition data store. The example retrieves credentials and uses them to access a data store.

This example is available on A2A Client Windows installations, in the `$CSPM_CLIENT_HOME\cloakware\cspmclient\examples\Csharp\IIS` directory:

File	Description
<code>ConnectionFactory.cs</code>	Class used to create an <code>SqlConnection</code> object. The object is used to connect to the data store and perform SQL queries.
<code>CspmClientComObject.cs</code>	Implementation of the <code>CSPMClient</code> interface. The class is used to retrieve the credentials from the Privileged Access Manager appliance.
<code>Connect.aspx</code>	ASP page used to open a connection to a data store. The page creates the <code>Connection</code> object using the <code>ConnectionFactory</code> class.
<code>Web.config</code>	Configuration file showing how to configure a connection string for SQL Server 2005 Express Edition. The connection string is passed to the <code>ConnectionFactory</code> class.

### Integration Process for IIS

Use the following procedure to modify your application to use Credential Manager to manage credentials.

#### Follow these steps:

1. Configure development environment. See [Configure your Development Environment for IIS](#).
2. Optionally, integrate the A2A Client to retrieve credentials. See [IIS Credential Viewer](#).
3. Create or modify the context file. See [IIS Connection with SQL Server 2005 Express Edition Data Store](#).
4. Register requestor. See [Register IIS Requestor](#).

### Deploy and Run the Sample IIS Application

Use the following procedure to compile and deploy the sample Web application using Visual Studio 2005.

#### Follow these steps:

1. Ensure IIS is running.
2. Open the IIS Manager and create a virtual directory called `iCSPM`.
3. Open Visual Studio 2005 with Visual C# 2005.
4. Build the solution.
5. Click `iCSPM` project.
6. Select `Publish iCSPM` to deploy the application to IIS.
7. Open a Web browser.

8. Load the following page: <http://localhost/iCSPM/>.

### **Configure your Development Environment for IIS**

You must configure your development environment for IIS development.

The example contains a Visual Studio 2005 project that you can use to build the Web application and to deploy it.

Use the following procedure to configure your environment for IIS development.

#### **Follow these steps:**

1. Install ASP.NET Framework 2.0. See <http://msdn2.microsoft.com/en-us/netframework/default.aspx>.
2. Ensure the Internet Information Service (IIS) is installed.  
Note: If the target server is running a 64-bit version of Windows, ensure the 32-bit version of the ASP.NET Framework is enabled.
3. Enable the 32-bit version of ASP.NET. Access <http://support.microsoft.com/kb/894435> and read section "ASP.NET 2.0, 32-bit version".
4. Install SQL Server 2005 Express Edition. See <http://msdn2.microsoft.com/en-us/express/bb410791.aspx>.
5. Ensure the Microsoft Visual Studio 2005 and Microsoft Visual C# are installed.

### **IIS Credential Viewer**

This example servlet shows you how to use the `CSPMClient` class to retrieve the credentials.

You create the `CSPMClient` class using a class factory.

#### ***Class File***

```
package com.cloakware.cspm.sample.web;

import java.io.IOException;

import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException; namespace iCSPM
{
    public partial class Default : System.Web.UI.Page
    {
        private const string ERR_MISSING_ALIAS = "Alias cannot be empty";

        protected void ViewBtn_Click(Object sender, EventArgs e)
        {
            // if the alias is missing
            if (aliasName.Text.Length == 0)
            {
                // Report the error
                errorMsg.Visible = true;
                errorMsg.Text = ERR_MISSING_ALIAS;
            }
            else
            {
                // Hide the error message field
                errorMsg.Visible = false;

                // Show the result table.
                resultTable.Visible = true;
            }
        }
    }
}
```

```
// Create CSPMClient COM Object
CspmClientObject obj;
if (useComObject.Checked)
{
obj = new CspmClientComObject();
}
else
{
obj = new CspmClientObject();
}

// Retrieve the credentials
Int32 statusCode = obj.RetrieveCredentials(aliasName.Text,
byPassCache.Checked ? "true" : "false", "");

// Initialize the return values.
returnCode.Text = statusCode.ToString();
returnMsg.Text = obj.GetStatusMsg(statusCode);
username.Text = obj.GetUserId;
password.Text = obj.GetPassword;

// Done with the object.
obj.Dispose();
}
}
}
```

## **IIS Connection with SQL Server 2005 Express Edition Data Store**

This example shows you how to create or modify a connection string used by the Credential ManagerConnectionFactory class. Use the ConfigurationManager class to retrieve the connection string from the Web.config file.

To integrate the A2A Client with your application, change the mechanism to create the connection. The Credential ManagerConnectionFactory retrieves the credentials using the A2A Client interface and then creates an SqlConnection object. In the Web.config file, you need to add the information regarding the alias to use. You add the alias as a parameter at the end of the connection string. The User ID and password parameters need to remain in the connection string as placeholders for the credentials, but leave them blank. The following is an example:

```
server=(local)\SQLEXPRESS;database=CSPMTest;uid=;pwd=;CSPMAlias=sql_svr
```

This management for connection acquisition means that all new connections obtained for a user whose database password has been changed (by the Credential Manager server) are made using the new password. This action occurs automatically without any knowledge or intervention by the owning connection pool.

While new connections are obtained using the new password, old connections that were obtained using an old password may linger in the connection pool. Also, if the Credential Manager alias is changed to a totally new user, then a connection pool has (at least temporarily) a mixture of connections for different actual database users.

Such connection management ensures that database password changes are completely transparent to connection activities.

The configuration file used in the example is located in %CSPM\_CLIENT\_HOME%\cloakware\csmpmclient\examples\Csharp\IIS.

## Data Source

```
<configuration>
<connectionStrings>
  <add name="CSPMSampleDS"
    connectionString="server=(local)\SQLExpress;
    database=CSPMTest;uid=;pwd=;
    CSPMAlias=sql_svr"
    providerName="System.Data.SqlClient"/>
</connectionStrings>
</configuration>
```

## Register IIS Requestor

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

Parameter	Description
Script Name	w3wp.exe
Execution Path	C:\WINDOWS\SysWOW64\inetsrv
Type	C

## Register SQL Server 2005 Express Edition as a Target Application

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

Parameter	Description
Application Name	SQL Server 2005 Express Edition
Application Type	MSSQL
Instance	SQLEXPRESS

Parameter	Description
Application	SQL Server 2005 Express Edition
Application Name	admin
Password	admin

Parameter	Description
Target Alias Name	sql_svr
Application	SQL Server 2005 Express Edition
Account	admin

## Integrate a Visual Basic, Java, or Windows Script

Scripts can be run from any application, such as Microsoft Internet Explorer.

## Visual Basic Script

This example uses a Visual Basic script sample (VBScriptSample.html ) in the \$CSPM\_CLIENT\_HOME \cloakware\cspmclient\examples\VB\_Script\_Sample directory. It uses the CA Technologies ATL DLL (cspmclientatl.dll ) to integrate the A2A Client.

### Code: Visual Basic Script

```
<html>
<head>
</head>
<body>
<script type="text/vbscript">

dim myobj
dim ret

set myobj = CreateObject("cspmclientatl.cspmclientatl")
document.write(" cspmclientatl dll is loaded. ")

ret= myobj.retrieveCredentials( "test","false", "whatever")
document.write(" The return value is: " & ret & ".")

ret= myobj.getUserId()
document.write(" User: " & ret & ",")

ret= myobj.getPassword()
document.write(" Password: " & ret & ",")

ret= myobj.getXMLData()
document.write(" XML data is: " & ret)
</script>
</body>
</html>
```

### Register Requestor - Visual Basic Script

See [Add and Run Credential Manager A2A Requestors](#) for the procedure to register your requestor with Credential Manager. Use the following data:

You need the following data to register your requestor with Credential Manager:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, VBScriptSample.html .
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, Visual Basic .

When entering the file and execution paths, you must specify the absolute paths without links. When an executable or script is run from a mapped network drive, Windows report the execution path using the UNC path. Use the UNC path when defining script path and execution path.

## Java Script

This example uses a Java script sample (JavaScriptSample.htm ) in the \$CSPM\_CLIENT\_HOME\cloakware\cspmclient\examples\Java\_Script\_Sample directory. It uses the CA Technologies ATL DLL (cspmclientatl.dll ) to integrate the A2A Client.

### Code: Java Script

```
<html>
<body>

<script type="text/javascript">
document.write("Client interface with Java Script");

try {
var XLApp = new ActiveXObject("cspmclientatl.cspmclientatl");

var retCode = XLApp.retrieveCredentials("test", "true", "no");
alert("The return code: " + retCode);
alert("The user name: " + XLApp.getUserId());
alert("The password: " + XLApp.getPassword());

} catch (e) {
alert("error: "+e.message);
}
</script>
</body>
</html>
```

### Register Requestor - Java Script

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

You need the following data to register your requestor with Credential Manager:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, JavaScriptSample.htm .
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, Java .

When entering the file and execution paths, you must specify the absolute paths without links. When an executable or script is run from a mapped network drive, Windows report the execution path using the UNC path. Use the UNC path when defining script path and execution path.

## Windows Script

This example uses a Windows script sample. It uses the CA Technologies ATL DLL (cspmclientatl.dll ) to integrate the A2A Client. Your installed A2A Client does not contain a soft copy of the following script.

### Code: Windows Script

```
Option Explicit

dim ret
```



```

dim cspmclient
dim credentialsRetrieved
dim success
dim bypasscache

'Instantiate the cspmclient
set cspmclient= CreateObject("cspmclientatl.ccspmclientatl")

'Retrieve the credentials using the cache first
bypasscache="false"
ret= cspmclient.retrieveCredentials( "test",bypassCache , "true")

if(ret = "400") then
WScript.Echo "accountName=" & cspmclient.getUserId()
WScript.Echo "password=" & cspmclient.getPassword()

'try to use it
'success = connectToApp(accountName,password)
success = false

'Retrieve credentials bypassing cache in the event of failure
if(success=false) then
bypasscache="true"
ret= cspmclient.retrieveCredentials( "test",bypassCache , "true")
if(ret = "400") then
WScript.Echo "accountName=" & cspmclient.getUserId()
WScript.Echo "password=" & cspmclient.getPassword()
'success = connectToApp(accountName,password)
else
WScript.Echo "Failed to retrieve credentials"
end if
end if
else
WScript.Echo "Failed to retrieve credentials"
end if
WScript.Quit

```

### **Register Requestor - Windows Script**

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension; for example, the name of the Windows script example given in [Windows Script](#).
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, WScript.

When entering the file and execution paths, you must specify the absolute paths without links. When an executable or script is run from a mapped network drive, Windows reports the execution path using the UNC path. Use the UNC path when defining script path and execution path.

## Integrate a PowerShell Script with A2A Client on Windows

The following PowerShell script uses Windows PowerShell to integrate the A2A Client (`cspmcclient.exe`). Your installed A2A Client contains a soft copy of the following 32-bit script and a 64-bit example.

### Code: PowerShell Script with A2A Client on Windows

```
#
# PowerShell (x86 32-bit) script example.
# To execute, do:
#   For 64-bit Windows system:
#   C:\> C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell %CSPM_CLIENT_HOME%\cspmcclient\examples\example.ps1 <A2A alias>
#   For 32-bit Windows system:
#   C:\> powershell %CSPM_CLIENT_HOME%\cspmcclient\examples\example.ps1 <A2A alias>
#
param([Parameter(Mandatory=$true)][string]$p1,
      [string]$p2="true")

if ($env:CSPM_CLIENT_HOME -eq $null) { Write-Host "Environment variable CSPM_CLIENT_HOME is not set"; exit }

$command = $env:CSPM_CLIENT_HOME + '\cspmcclient\bin\cspmcclient.exe' + ' ' + $p1 + ' ' + $p2
$output = Invoke-Expression $command
$tokens = $output.split(' ')
$rc = $tokens[0]
$userid = $tokens[1]
$password = $tokens[2]
Write-Host "Return Code:" $rc
Write-Host "User ID:" $userid
Write-Host "Password:" $password
```

### Register Requestor - PowerShell Script with A2A Client on Windows

See [Integrate Applications with the Credential Manager A2A Client](#) for the procedure to register your requestor with Credential Manager. Use the following data:

- Script name. The name of the requestor file that contains the Credential Manager executable call including the file extension. For example, the name of the PowerShell script example given in [Code: PowerShell Script with A2A Client on Windows](#).
- File path. The absolute path to the application file that contains the executable call.
- Execution path. The absolute path from which the application is launched.
- Script type. The requestor script type; for example, PowerShell.

When entering the file and execution paths, you must specify the absolute paths without links.

## Remote HTTP Interface to a Credential Manager A2A Client

The A2A Client supports HTTP requests for credentials. You can retrieve credentials of a target account alias by entering a URL in your Web browser.

Access the URL to see the credentials in the following cases:

- Only the local host (where the A2A Client is installed). See [Access URL from only the Local Host](#).
- Only the systems within the network of the local host. See [Access URL from Local Host Network](#).
- Both the local host and the systems within its network. See [Access URL from Local Host and Local Host Network](#).

To enable this functionality, add the `httpRequestScriptAddress` tag and the `httpRequestScriptPort` tag in the client configuration file. The configuration file is named `cspm_client_config.xml`. It is located in the `$CSPM_CLIENT_HOME/cspmclient/config` directory. After you add the tags, restart the A2A Client daemon (on UNIX) or the A2A Client service (on Windows).

To disable this feature, remove or comment out the `httpRequestScriptAddress` tag and the `httpRequestScriptPort` tag in the `cspm_client_config.xml` file.

The following XML code is an example of the `cspm_client_config.xml` file with the tags.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<applicationtype>cspm</applicationtype>
<cacheallow>true</cacheallow>
<loglevel>FINE</loglevel>
<cspmserver>rh5x32stout2.cpa.intra</cspmserver>
<cspmserver_port></cspmserver_port>
<httpRequestScriptAddress>0.0.0.0</httpRequestScriptAddress>
<httpRequestScriptPort>12345</httpRequestScriptPort>
<daemonserver1_port>28088</daemonserver1_port>
<daemonserver2_port>28888</daemonserver2_port>
<logfile>/opt/cloakware/cspmclient/log/cspm_client_log.txt</logfile>
<c_logfile>/tmp/cspm_c_client_log.txt</c_logfile>
<patch>
<frequency>daily</frequency>
<starthour>0</starthour>
<endhour>5</endhour>
</patch>
<operation>production</operation>
</configuration>
```

To authorize a requestor (script) to retrieve credentials through a URL, the authorization mappings between the target alias and the request server must contain at least one script that produces URLs with the formats described in the following sections. See [Configure A2A Authorization Mappings](#) for more details on authorization mapping.

### **Access URL from Only the Local Host**

This case enables access from only the local host system where the A2A client is installed.

For this case, add the following tags to the `cspm_client_config.xml` file:

- `<httpRequestScriptAddress>localhost</httpRequestScriptAddress>`  
You can also specify the loop back IP address of the local host instead of the literal term `localhost`. For example, the following tags are equivalent:
  - `<httpRequestScriptAddress>127.0.0.1</httpRequestScriptAddress>` (IPv4),  
or `<httpRequestScriptAddress>::1</httpRequestScriptAddress>` (IPv6)
  - `<httpRequestScriptAddress>localhost</httpRequestScriptAddress>`
- `<httpRequestScriptPort> <port_no> </httpRequestScriptPort>`, where **<port\_no>** is the port number of the local host. The following tag is an example:
  - `<httpRequestScriptPort>12345</httpRequestScriptPort>`

For this case, use the following URL format on the local host system to get credentials:

`http:// <system> : <portnumber> /requestScript/retrieveCredentials?aliasName= <targetalias> &bypassCache=false&contentType=html`, where:

- **<system>** is the literal term `localhost` or the loop back IP address of the local host. This must match what was specified in the `<httpRequestScriptAddress>` tag for the A2A client on the system.
- **<portnumber>** is any valid and unused port number of the local host. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- **<targetalias>** is the target alias for which credentials must be fetched

The following URL is an example:

```
http://127.0.0.1:12345/requestScript/retrieveCredentials?
aliasName=testalias&bypassCache=false&contentType=html
```

### **Access URL from Local Host Network**

This case enables access from only the systems that share the local network of the local host, but not from the local host itself.

For this case, add the following tags to the `cspm_client_config.xml` file:

- `<httpRequestScriptAddress><myhostname>.<mydomain></httpRequestScriptAddress>`
  - **<myhostname>** is the host name or the loop back IP address of the system where the A2A Client is installed
  - **<mydomain>** is the domain of the system where the A2A Client is installed
- `<httpRequestScriptPort> <port_no> </httpRequestScriptPort>` , where **<port\_no >** is any valid and unused port number of the system where the A2A Client is installed

For this case, use the following URL format on any system on the local network of the local host to get credentials:

```
http:// <myhostname> . <mydomain> : <portnumber> /requestScript/retrieveCredentials?
aliasName= <targetalias> &bypassCache=false&contentType=html , where:
```

- **<myhostname>** is the host name or the loop back IP address of the system where the A2A Client is installed. This must match what was specified in the `<httpRequestScriptAddress>` tag for the A2A client on the system.
- **<mydomain>** is the domain of the system where the A2A Client is installed. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- **<portnumber>** is port number to access the local host. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- **<targetalias>** is the target alias for which credentials must be fetched

The following URL is an example:

```
http://rh5x32stout.cpa.intra:12345/requestScript/retrieveCredentials?
aliasName=testalias&bypassCache=false&contentType=html
```

In the previous example:

- `rh5x32stout` is the host name of a system that shares the local host network
- `cpa.intra` is the domain of the system where the A2A Client is installed
- `12345` is port number to access the local host. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- `testalias` is the target alias for which credentials must be fetched

### **Access URL from Local Host and Local Host Network**

This case enables access from the systems that share the local network of the local host and from the local host itself.

For this case, add the following tags to the `cspm_client_config.xml` file:

- `<httpRequestScriptAddress> 0.0.0.0 </RequestScriptAddress>`
- `<httpRequestScriptPort> <port_no> </httpRequestScriptPort>` , where **<port\_no>** is any valid and unused port number of the system where the A2A Client is installed

For this case, use the following URL format on the local host system to get credentials:

`http:// <system> : <portnumber> /requestScript/retrieveCredentials?aliasName= <targetalias> &bypassCache=false&contentType=html` , where:

- **<system>** is the literal term `localhost` or the loop back IP address of the local host
- **<portnumber>** is any valid and unused port number of the local host
- **<targetalias>** is the target alias for which credentials must be fetched

For this case, use the following URL format on any system on the local network of the local host to get credentials:

`http:// <myhostname> . <mydomain> : <portnumber> /requestScript/retrieveCredentials? aliasName= <targetalias> &bypassCache=false&contentType=html` , where:

- **<myhostname>** is the host name or the loop back IP address of the system where the A2A Client is installed.
- **<mydomain>** is the domain of the system where the A2A Client is installed.
- **<portnumber>** is port number to access the local host. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- **<targetalias>** is the target alias for which credentials must be fetched

The following is an example of the URL to use from the local host system to get credentials:

`http://127.0.0.1:12345/requestScript/retrieveCredentials?`  
`aliasName=testalias&bypassCache=false&contentType=html` (IPv4), or  
`http://[::1]:12345/requestScript/retrieveCredentials?`  
`aliasName=testalias&bypassCache=false&contentType=html` (IPv6)

The following is an example of the URL to use from a system on the local network of the local host to get credentials:

`http://rh5x32stout.cpa.intra:12345/requestScript/retrieveCredentials?`  
`aliasName=testalias&bypassCache=false&contentType=html`

In the previous example:

- `rh5x32stout` is the host name of a system that shares the network of the local host
- `cpa.intra` is the domain of the system where the A2A Client is installed
- `12345` is port number to access the local host. This must match what was specified in the `<httpRequestScriptPort>` tag for the A2A client on the system.
- `testalias` is the target alias for which credentials must be fetched

## Reference

---

This section contains reference information about the PAM Client, Target Connectors, Messages, Logs Formats, and more. Use the table of contents to access the content.

### Privileged Access Manager Client Reference

The PAM Client enables you to log in to Privileged Access Manager and perform administrator and end-user activities without a customer-installed Web browser and Java engine. The PAM Client removes the maintenance that is required to keep Java and browser configurations compatible with Privileged Access Manager.

#### Installer

Run the installer file to provide a CA PAM Client instance on your workstation.

#### **Download Buttons**

From your client workstation, download an installer from the Privileged Access Manager login page. Point to Privileged Access Manager from an approved browser, and from the GUI login page, select **Symantec PAM Client**. Click to open a drop-down list and select a specific version for your OS type.

#### **Installer Program**

Run the installer file to open its InstallAnywhere wizard.

Set the installation parameters according to its interface.

- **License Agreement** – The acceptance button is activated only after you scroll the license text to the bottom of the panel.
- **Choose Install Set** – Select one of the following options:
  - **Typical**: install the client on the local workstation or
  - **Run**: The contents are extracted only to a temporary location and executed.
- **Installing...** – You cannot select **Previous** after the software starts installation or has completed it.

#### **Silent Installation**

For instructions on using the silent install feature, see [PAM Client Silent Install](#).

#### Client

Run the CA PAM Client program to access the following interfaces. From the client window, you can:

- Continue to the login screen, to the console screen or browser window
- Open the Configuration Settings window, or the About window, or the browser window

#### **Configure Settings**

The **Show settings dialog** gear icon opens the **Configuration Settings** window, with settings on the following tabs:

- **Proxy**: When applicable, identify the client proxy.
- **General**: You can set client memory size, change the client language, or restore security prompts. Select **Restore** to reverse a previous "Ignore host mismatch for this address" selection that is made in a **Verify Certificate** pop-up window during connection.
- **Cache**: Set and manage the client cache size.
- **Certificate**: Select an applicable security certificate, or import one.

The **Show About dialog** question mark icon opens the **About CA Privileged Access Manager** window, which has information about the client release level.

The Settings and About dialogs cannot be open simultaneously.

### **Connect**

To connect to a Privileged Access Manager instance, follow these steps:

1. Select its **Address**.

#### **NOTE**

If you enter an IPv6 address, make sure to enclose the address in brackets. If you want to enter a port number with the IPv6 address, add a colon, followed by the port number. For example:

[2001:db8:3333:4444:5555:6666:7777:8888]:443

2. Select a **Connect Mode**:

- a. **WEB** mode checks for client updates, and processes an update if one is found. It then opens a connection to the Privileged Access Manager server, and opens the PAM Client browser window, and closes the console.
- b. **CONNECT** mode checks for client updates, and processes an update if one is found. It then opens a connection to the Privileged Access Manager server, and maintains a status connection window. The PAM Client browser window can be opened from the status window.

You may receive a Verify Certificate window before the login screen appears.

3. On the Login screen, enter the appropriate values in the following fields, and select **Login**:

- a. **User**
- b. **Password**
- c. **Authentication Type**

Upon login, you are first presented with a console window or browser window, depending on your earlier **Connect Mode** choice.

- a. If you used **CONNECT**, the console screen takes the place of the login screen. This screen displays connections statistics, and allows you to **Launch Web Browser** or **Log Off**.
  - b. If you used **WEB**, CA PAM Client browser window appears without the connection information.
4. The browser window displays the traditional GUI, and its features operate in the same way. When you log out from the GUI in the browser window, you return to the login screen.

## **Data Formats**

The content in this section describes data formats that are used by Privileged Access Manager.

### **Multi-Byte Character Support**

#### ***Managed Object Names***

- Username in a User record that inherits from Import LDAP Users
- Groupname in a User Group record
- Device Name in a Device record
- Group Name in a Device Group record
- Application Name in a Target Application record
- Account Name in a Target Account record

#### ***Message Templates***

- License acceptance (at Login) – configured in Show License Warning in Global Settings
- Session recording warning – configured in Show Recording Warning in Global Settings
- Blacklist violation – configured in Blacklist Violation Message in Policies > Manage Policies: Manage Filters > Command Filter Config
- Whitelist violation – configured in Whitelist Violation Message in Policies > Manage Policies: Manage Filters > Command Filter Config

## **Port Numbers**

### **General Syntax**

Use the following conventions to represent port values when populating Privileged Access Manager GUI fields:

**All ports** (or, where the port number is not relevant)

\* = ("is equivalent to") Ports 1 through 65535, inclusive

all = ("is equivalent to") Ports 1 through 65535, inclusive

ALL = ("is equivalent to") Ports 1 through 65535, inclusive

**Specific ports** (a sequence of one or more port numbers that are delimited by spaces or commas)

X Y = Ports X and Y [and Z [...]]

Example: 2 3 18 39230 = Ports 2, 3, 18, and 39230

**Port Forwarding** (Port Mapping)

X:Y = (Remote) port X is mapped (or forwarded) to (local) port Y

Example: 345:1223 = Port 345 is forwarded to port 1223

**Port Range**

X-Y = Ports X through Y, inclusive

Example: 6-10 = Ports 6, 7, 8, 9, and 10

### **NOT PERMITTED**

Combination syntax cases such as those in the following examples have undefined values and, thus, are not permitted in Privileged Access Manager GUI fields:

X-Y:U-V does not mean: Port X through Y -onto- port U through V

X:Y U:V does not mean: Port X onto Y -and- port U onto V

Thus, the X-Y-U-V combinations that are shown above **must not be used**.

### **Rules for Specific Interfaces**

#### **Access page connection-method links:**

Pop-up window: Application path specification field, ports as specified in Service Definition

**Global Settings** editing fields:

**Access Methods:** *Each field:* One port only • No Range, No Mapping

**Services > TCP/UDP Services** editing fields:

**Basic Info:** Specific ports -or- one Range, with 1-500 ports -or- one Mapping

**> SSLVPN** editing fields:

**Basic Info:** All ports -or- Specific ports -or- one Range, with 1-500 ports -or- one Mapping



**Devices > Manage Devices** editing fields:

**Special Type:** Specific ports -or- one Range, with 1-500 ports • No Mapping

**Access Methods:** One port only • No Range, No Mapping

**Policies > Manage Policies :** Manage Filters > Socket Filter Config editing fields:

One port only • No Range, No Mapping

**> Socket Filter Lists** editing fields:

All ports -or- Specific ports -or- One Range • No Mapping

### Session Recording File Names

The session recording files on a storage share are named according to the following format: `H-NT.ext`

Where...	Example
H = Privileged Access Manager Hostname:	capam123
N = (Pseudorandom) ID number:	8732209813
T = Start Time of Recording: YYYYMMDDHHMMSSXXX	20120125145538987
“XXX” represents the millisecond resolution of the start time. If there is a collision with an existing file, this number is incremented by 1 until an available filename is found.	
ext = File Type Extension:	for a CLI session recording: <code>txt</code> for an RDP session recording: <code>gsr</code> for a VNC session recording: <code>vsr</code>

For example, the file name `capam123-873220981320120125145538987.txt` identifies a CLI recording file for appliance host `capam123` that was assigned ID number `8732209813` and is timestamped January 25, 2012 at 2:55:38.987 PM.

## Import and Export Data for Provisioning

This section describes how to import and export data from Privileged Access Manager for provisioning.

### File Imports

PAM-managed objects may be imported only from comma-separated value (CSV) files.

#### **File Import Preparation**

CSV files can be created in many text editors or spreadsheet programs and saved as plain text. If you support special characters such as UTF-8 (for example, Cyrillic or Chinese), confirm that your application supports them. Your version of Microsoft Excel® or Google Drive, for example, may or may not have that support.

You may want to use the provided sample files as templates and refer to the information in the following pages to populate the fields.

#### **File Import Process**

To handle attribute dependencies when provisioning multiple PAM objects using CSV files, import the files in the following order. You can use any file name, as long as you save the file in plain text with the CSV file extension.

Import CSV files by selecting the **Import/Export** button on the corresponding import page (identified in the following table) to perform object-specific error checking.

Import order	Managed Objects in File	Import/Export Page Location
1	Web Proxies	<b>Configuration, Network, Web Proxies</b>
2	Transparent Login	<b>Services, Transparent Login Configurations</b>
3	TCP/UDP Services	<b>Services, TCP/UDP Services</b>
4	Roles	<b>Users, Manage Roles</b>
5	User Groups, then Users	<b>Users, Manage User Groups</b> <b>Users, Manage Users</b>
6	Device Groups, then Devices	<b>Devices, Manage Device Groups</b> <b>Devices, Manage Devices</b>
7	Vaults	<b>Secrets, Manage Vaults</b>
8	Socket Filter Lists	<b>Policies, Manage Policy Filters, Socket Filters tab</b>
9	Command Filter Lists	<b>Policies, Manage Policy Filters, Command Filters tab</b>
10	Policies	<b>Policies, Manage Policies</b>

### ***File Import Content Considerations***

When importing files, consider the following constraints:

- CSV file fields are comma-separated. To use a comma in field content, surround the field with quotation marks (").
- CSV files that contain user group and user data must list them in that order. That is, the file must list all user groups before listing users.
- CSV files containing device group and device information must list them in that order. That is, the file must list all device groups before listing devices.
- Not all record content must be imported to create a record – the tables identify with asterisks \* which fields are required for particular record types.
- The first line in each file is for column names, which are used to identify record fields during import.
- CSV file columns may be rearranged as long as the corresponding CSV File Column Labels are preserved.
- After you import, you can check the results by clicking the Download CSV Import Results link that appears after the import, below any error messages.

### **File Export**

#### ***Exported File Names and Types***

Each exported file is downloaded with a timestamp in the file name according to the following syntax:

objecttypeYYYYMMDDHHMMSS.csv

Example: **devices20110715131849.csv**

#### ***Exported File Content Considerations***

When exporting files, consider the following facts:

- Several informational fields are added to a Users Group/Users export file. The export does not preserve the import column arrangement (they are inserted between field columns). These informational fields are identified in the tables by oblique names.
- Privileged Access Manager does not display stored passwords in User record exports. Each cell in the Password column (which is used only for imports) is empty.

## Transfers

CSV files are frequently used to transfer (export and import) from one PAM server to another.

### LDAP Users

LDAP user records draw data from two locations: fields from the LDAP source directory and any data to CA PAM-specific fields the administrator may add after the LDAP import.

To perform an LDAP transfer, recreate a baseline LDAP import, and then “overlay” the PAM fields:

1. At the source PAM server, **Export Users** to a CSV file.
2. At the destination PAM server, **Import LDAP Group** from the source LDAP directory(ies).
3. At the destination PAM server, **Import Users** with the CSV file obtained from the source Privileged Access Manager.

### Specific CSV File Formats

For details about specific types of CSV import and export format, use the table of contents to access the other topics in the section.

## Roles

In **Users, Manage Roles, Import/Export**, you can download a sample file and can populate it according to the specification in the following table.

In Record Type, \* = required. This import allows you to *create* roles – you are not limited to the set of preconfigured roles (such as “Auditor” and “Troubleshooter”).

CSV File Column Label	Permitted Values	Description / Notes
Type	role	Import record (row) type
Role Name	text*	Name of the Role
Description	text	Role description or other information
Role Privileges	text	Role privileges (not case-sensitive). The list of valid role privilege names can be retrieved from the Manage Roles page in the GUI. Multiple privileges are separated by:   (pipe)

## User Groups and Users

Import Users and User Groups from a specially formatted *User Import CSV file* using the controls from the **Users, Import/Export Users** page in the GUI.

### Export Users and User Groups to a CSV File

You can export your existing Users and User Groups to a User Import CSV file.

#### Follow these steps:

1. Go to **Users, Manage Users**.
2. Select the **Import/Export** button.
3. Select the **Export Users (User Groups)** button.

A CSV file of existing Users and User Groups is prepared and saved to your local drive. The default filename is usersYYYYMMDDHHSS.csv

## Download a Sample Import CSV File

To download a sample User Import CSV file, go to **Users, Manage Users**. Select **Import/Export**, and then select **Download Sample File**.

## Add Users and User Groups to the Import CSV File

To define Users and User Groups to import, add appropriate entries to the User Import CSV file.

### NOTE

For Users provisioned in an external repository (such as AWS or VMware), do *not* modify any field that was sourced from the external repository. For example, for LDAP users, do not change the User Principle Name (or other LDAP-sourced) fields.

The following table describes the fields in the User Import CSV file.

### How to read the table:

- **Bold** text (aside from table column labels) indicates either literal values to be entered into fields or literal values or legends that are displayed by the GUI or present in export files.
- **Table Columns:**
  - **CSV File Column Label**
    - Rows are shown here in the same order as the columns in the sample file.
    - Column order is not recognized by import processing – only the items in CSV File Column Labels are.
    - *Italic* text indicates columns that are generated solely for export files – they are not required in files for import.
    - Ensure that all required columns (with a \* in the Record Type column) are included in the CSV file.
    - Ensure that column headers are spelled as noted in CSV File Column Label or their values will not be imported.
    - Ensure that no (embedded) blank columns exist.
  - **Record Type**= Type of import record:
    - **U** = for inclusion in imported User record
    - **UG** = for inclusion in imported User Group record
    - **E** = data that is provided by Privileged Access Manager in an exported file (and not required in the import file)
    - \* = Indicates that this field is required to create a record of this type. (This does not identify what is necessary to function, however.)
  - **Description**
    - This column lists User or User Group label that differ from the corresponding column name for the import file.

CSV File Column Label	Record Type	Permitted Values	Description / Notes
Type	U* UG*	user, user group	Import record (row) type
UserName	U* UG*	text	User ID for login User record label: One of <b>Username</b> or <b>User Group ID</b> User Group record label: One of <b>Groupname</b> or <b>LDAP: DN</b>
<i>ShortName</i>	E		CN
First Name	U*	text	User first name. User record label: <b>Firstname</b>

Last Name	U*	text	User last name. User record label: <b>Lastname</b>
Password	U*	text	Plain text User password. <b>Note:</b> Users are forced to change their passwords at first login.
<i>Password Set Time</i>	E	UNIX timestamp	
Phone	U	text	User telephone number
Cell Phone	U	text	User mobile telephone number
Email	U*	text	Valid email address User record label: <b>e-mail</b>
Description	U UG	text	User or User Group description or other information
Active Flag	U	<b>f</b> = Disabled <b>t</b> = Enabled (Do not use uppercase 'F' and 'T') GUI default value: <b>f</b>	<b>Note:</b> This field is not related to GUI field "Activate Account" User record label: Account Status
Activation Time	U	UNIX timestamp GUI default value: 0	Account activation date. If empty, account will be activated after import. User record fields: Activate Account=Later (default=Now) ...triggers display of: Account Activation (= CSV label "Activation Time")
<i>Last Activation Time</i>	E	UNIX timestamp	
<i>Account Disabled Time</i>	E	UNIX timestamp	
Expiration Time	U	UNIX timestamp GUI default value: 0	Account expiration date. If empty, account never expires. User record label: <b>Account Expiration</b>
Authentication	U UG	One of: • local • ldap • radius • tacacs+ GUI default value: <b>local</b>	User or User Group Authentication type
Email on Login Contact	U	text	Send notification to this email address upon login by this user. User record label: <b>Email on Login</b>

Email Self on Login Flag	U	<b>f</b> = Disabled <b>t</b> = Enabled (Do not use uppercase 'F' and 'T') GUI default value: <b>f</b>	Send notification to this user by email upon their login. User record label: <b>Email Self on Login</b>
Terminate Session on Deactivation Flag	U	<b>f</b> = Disabled <b>t</b> = Enabled (Do not use uppercase 'F' and 'T') GUI default value: <b>f</b>	User record label: <b>Terminate session upon deactivation</b>
Access Times	U UG	<p>Each entry takes the following form:</p> <p><i>day=SMTWTFS timeFrom=minutes timeTo=minutes</i></p> <p><b>SMTWTFS</b> Specifies the days of the week where access is permitted. Each day where access permitted is represented by a "1" and each day where access is not permitted is represented as a "0"</p> <p><i>timeFrom</i> Specifies the number of minutes from midnight the time when access should start.</p> <p><i>timeTo</i> Specifies the number of minutes from midnight to the time when access should end.</p> <p>Example: An entry of day=0111110 timeFrom=480 timeTo=1080 means "Monday through Friday, from 8:00 AM to 6:00 PM"</p> <p>User record label: <b>Access Time : Access Days + From (time) + To (time)</b></p>	
Group Membership	U	text	User Group or User Groups of which the user is a member. Separate multiple User Groups with a   (pipe) character.
Applet Message	UG	<b>f</b> = Disabled <b>t</b> = Enabled (Do not use uppercase 'F' and 'T') GUI default value: <b>f</b>	Enable/Disable the Global Settings: Warnings: Show Recording Warning to this group User Group record label: <b>Applet Recording Warning</b>
Provision Type	E	One of: <ul style="list-style-type: none"> <li>• local</li> <li>• ldap</li> <li>• virtual</li> <li>• radius</li> <li>• pki</li> <li>• saml</li> </ul>	Source of the User or User Group information. Do <i>not</i> change this value if it is populated from an export. For new Users, use <b>local</b> .

Roles	U UG	<p>Syntax (in CSV cell, the string shown without quotes, either with value substitutions as shown, or without one or more values):</p> <p><b>"roleName=roleName roleUserGroups=roleUserGroups roleDeviceGroups=roleDeviceGroups"</b>.</p> <p>Separate adjacent role specifications with a comma.  <i>roleName</i> = Choose from the built-in and administrator-defined Access roles. GUI default value: <b>"Standard User"</b>  <i>roleUserGroups</i> =  <i>roleDeviceGroups</i> =</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• roleName=Auditor roleUserGroups=roleDeviceGroups=</li> <li>• roleName=Global Administrator roleUserGroups=ALL roleDeviceGroups=ALL</li> </ul> <p>User / User Group record label: Available Roles</p>	
Smart Button Group	N/A	N/A	Obsolete. Maintained for backward compatibility only.
User Principle Name	E		Extracted from LDAP record (where applicable)
PA Group Membership	U	text (matching existing name)	The names of Credential Manager User Groups of which the user is a member, where each pair of User Group names is separated by: " " (pipe) character.
Login IP Ranges	UG	Valid IP Ranges for User in this Group	Example: 10.1.10.0/24, 10.7.0.0/16 (IPv4) or fd6d:8d64:af0c:1:0:242:22:233/80, fd6d:8d64:af0c:1:0:242:22:233/64 (IPv6)

API Keys	U only	<p>Each API Key cell has values that are represented by the following fields:</p> <pre> name=apiKeyName isActive=[t f] description=descriptionOfApiKey roles=rolename=rolename1OfApiKey1 [, rolename=rolename2OfApiKey1 [, ...]] [#&amp; rolename=rolename1OfApiKey1 [, rolename=rolename2OfApiKey1 [, ...]] [ ... ]]</pre> <p>Delimited with:</p> <pre> "before cell string , (space+comma) between each pair of roles in a key /; between each pair of fields in cell API Keys  #&amp; between each pair keys in field roles "after cell string</pre> <p>EXAMPLE:</p> <pre> "name=test123/;isActive=t/;description=Test 123. description./;roles=roleName=Service Manager roleUserGroups= roleDeviceGroups=. , roleName=Password Manager roleUserGroups=. roleDeviceGroups=#&amp;name=test234/;isActive=t/; description=Test 234. description./;roles=roleName=Service Manager roleUserGroups= roleDeviceGroups=. , roleName=Password Manager roleUserGroups= roleDeviceGroups="</pre>
----------	--------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**NOTE**

In the **Roles** field, do *not* assign any User **solely** the role "Password Manager". That role does not contain sufficient privileges for Privileged Access Manager access. Instead, when you intend to allow only password management privileges, add the role "Standard User" using Credential Manager. (Standard User is the default role that is populated in a newly created Privileged Access Manager user template.)

**Import Users and User Groups**

You can import Users and User Groups from an appropriately formatted User Import CSV file,

**Follow these steps:**

1. Go to **Users, Manage Users**.
2. Select the **Import/Export** button.
3. Select **Choose File**, find the file to import, and select **Open** in the **File Upload** dialog that appears.
4. Select **Import Users (User Groups)**.



## Device Groups and Devices

You can download a sample CSV file that defines devices. You can customize that file for your devices and then import or export the file (Devices, Manage Devices, Import/Export) for configuration purposes.

The following table lists the contents of the CSV file and the values that you can specify for each entry.

### TIP

In the **Record Type** column of the table, an asterisk indicates whether the entry is required for a Device (D), or a Device Group (DG).

Column Label	Record Type	Permitted Values	Description/Notes
Type	D* DG*	device or device group	Import record (row) type
DeviceName	D* DG*	text	Name of the Device or Device Group record label: Group Name
Address	D*	IP address or FQDN	Network location
Special Type Flag			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Special Type Type			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Special Type Login			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Special Type Password			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Special Type Protocol			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Special Type Ports			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Operating System	D	Enumerated options: <ul style="list-style-type: none"> <li>AIX BeOS FreeBSD</li> <li>HP-UX Linux NetBSD OpenBSD Other Solaris</li> <li>Embedded OS</li> <li>IBM AS/400</li> <li>Mac OS 9</li> <li>Mac OS X</li> <li>IBM Mainframe</li> <li>SCO UNIX</li> <li>Windows 2008</li> <li>Windows Vista</li> <li>Windows 7</li> <li>Windows Desktop</li> </ul>	Operating system of Device (Does not currently allow custom options)
Location	D	text	Device location (description)
FTP Mode	D	1	

Description	D DG	text	Device or Device Group description or other information
Access Methods	D		<p>Use the following template for each Access Method:  <b>'name=name custom_name=custom_name port =port property=property'</b></p> <p>Place holder options are:</p> <ul style="list-style-type: none"> <li><b>name:</b> VNC, Telnet, SSH, RDP If mainframe licensing is enabled, name options: TN3270, TN3270SSL, TN5250, TN5250SSL</li> <li><b>custom_name:</b> (optional) any string</li> <li><b>port:</b> Range for one port (only) is 0-65535. For VNC: leave empty or enter 0 if disabled</li> <li><b>property:</b> (empty); NULL</li> </ul> <p>Separate multiple access methods with the   (pipe) character.</p>
	D DG	VNC, Telnet, SSH, RDP	Access Method category (no specific access information)
Services	D DG	<p>Custom Services, or Built-in Services:</p> <ul style="list-style-type: none"> <li>sftpftp</li> <li>sftpftpemb</li> <li>sftpstftp</li> <li>sftpstftpemb</li> <li>TSWEB</li> </ul>	Specify built-in or custom Services. Separate any multiple Services by:   (pipe)
OOB Serial Host Flag			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
OOB Serial Host			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
OOB Serial Port			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
OOB KVM Host Flag			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
OOB KVM Host			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
OOB KVM Port			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Power			DEPRECATED - Do not remove the column, but do not use it. Applicable to the out-of-band (OOB) device types.
Term Type	D	<ul style="list-style-type: none"> <li>ansi</li> <li>ibm</li> <li>scoansi</li> <li>vt100</li> <li>vt220</li> <li>vt320</li> <li>xterm</li> </ul>	Specify one terminal type
Term Key Mapping	D	<ul style="list-style-type: none"> <li>puttyDefault</li> <li>AT386.conf</li> <li>vt320.conf</li> </ul>	Specify one from allowed values
Term Customization	D	<p><b>0</b> = do not use settings</p> <p><b>1</b> = use settings</p>	Flag to use terminal customization settings: Term Character Encoding through Term End Select

Term Character Encoding	D	<ul style="list-style-type: none"> <li>UTF-8</li> <li>ISO-8859-1</li> </ul> (many other options)	Terminal character encoding type. (See GUI for full list, or Administration Guide for list and information.)
Term Font Family	D	<ul style="list-style-type: none"> <li>Monospaced</li> <li>Courier</li> <li>Courier New</li> </ul>	Select one from allowed values
Term Font Size	D	8–32	Terminal font size
Term Cursor Foreground	D	RGB hex triplet Example: #000000 (Black)	Cursor foreground color
Term Cursor Background	D	RGB hex triplet Example: #FFFFFF (White)	Cursor background color
Term Foreground Color	D	RGB hex triplet Example: #FFFFFF (White)	Foreground color
Term Background Color	D	RGB hex triplet Example: #000000 (Black)	Background color
Term Terminal Size	D	[width, height] in pixels Example: [80,24]	Terminal window size NOTE: Include brackets in setting.
Term Buffer Size	D	integer	Buffer size in bytes
Term Scroll Position	D	left or right	Select one from allowed values
Term End Select	D	0 or 1	Flag to use “End” to select
Device Monitor			DEPRECATED - Do not remove column, but do not use it. Applicable to deprecated Device Monitoring feature.
Tags	D	text	Free-form text attributes (zero or more) can be assigned to any device. Embedded spaces are allowed. Separate each pair of tags by:   (pipe)
Type Access	D	<b>f</b> = False <b>t</b> = True	Marker for an Access type Device
Type Password	D	<b>f</b> = False <b>t</b> = True	Marker for a Password Management type Device
Type A2A	D	<b>f</b> = False <b>t</b> = True	Marker for an A2A type Device
Target Server Description 1	D	text	If Type Password = t, this option is available
Target Server Description 2	D	text	If Type Password = t, this option is available
Request Client Description 1	D	text	If Type A2A = t, this option is available
Request Client Description 2	D	text	If Type A2A = t, this option is available
Request Client Active	D	<b>f</b> = False <b>t</b> = True	If Type A2A = t, this option is available
Host Name Preserved	D	<b>f</b> = False <b>t</b> = True	If Type A2A = t, this option is available

ProvisionType	DG	0 - 4	The provision type of the Device Group: 0 = Local 1 = AWS 2 = VMware 3 = LDAP 4 = Azure
AlternateId	D	text	Only a virtual Device can have an AlternateID .
Group Membership	D	text	Groups that the Device is member of, separated by:   (pipe) Device record label: Available Groups
Credential Source Name	DG	text	Separate multiple credential source names with the   (pipe) character.
Password Push	DG	1 = Enabled 0 = Disabled	This setting is maintained by a checkbox on the Enabled tab of the Device Group window: Provide Credentials for "Always Prompt for Password"
Override Address	D	f = False t = True	Applicable only to provisioned virtual devices.
Transparent Login Parameters	D	text	This setting resides on the Transparent Login tab of the Device. It combines the <b>Full Path To</b> and the <b>Password Prompt</b> for the <code>sudo</code> and <code>pbrun</code> commands. The command values are separated by a pipe, and the path from the password prompt by a semicolon. For example: <code>/etc/sudo;su /ext/pbrun;pwd</code>
Transparent Login Type	D	None or sudo/pbrun	This setting resides on the Transparent Login tab of the Device.
Handle Legal Notice	DG	1 = Enabled 0 = Disabled	This setting is maintained by a checkbox on the Enabled tab of the Device Group window: Handle "Legal Notice" on Logon screen.
Kerberos KDC server	D DG	IP address of a configured KDC server	This setting resides on the KDC Server tab of the Device.

## CSV Files for Services

In Services, Import/Export Services, you can download a sample file and can populate it according to the specifications in the following table. In Record Type, \* = required for that type of record (TCP/UDP, TCP/UDP: Web Portal, SSL VPN, or Application).

CSV File Column Label	Record Type	Permitted Values	Description / Notes
Type	All*	TCP/UDP Application	Import record (row) type
Service Name	All*	text	Name of the service Application record label: <b>App Name</b>
Local IP	TCP*	IPv4 local address or ' : : 1 ' for IPv6 address	The local IP address of this service. Must be on the Class A 127 network.

<b>TCP Ports</b>	TCP SSL	Port value	<p>The service TCP ports. Either:</p> <ul style="list-style-type: none"> <li>One or more port numbers that are separated by space or comma</li> <li>One port range with 1-500 port</li> <li>One port mapping</li> </ul> <p>For TCP/UDP services, if a value is specified for both TCP Ports and UDP Ports, the values must match exactly. For both types of services, a port value is required for at least one of TCP Ports and UDP Ports.</p> <p>TCP/UDP Service record labels: <b>Port(s) + Protocol</b></p>
<b>UDP Ports</b>	TCP SSL	Port value	<p>The service UDP ports. Either:</p> <ul style="list-style-type: none"> <li>One or more port numbers that are separated by space or comma</li> <li>One port range with 1-500 port</li> <li>One port mapping</li> </ul> <p>For TCP/UDP services, if a value is specified for both TCP Ports and UDP Ports, the values must match exactly. For both types of services, a port value is required for at least one of TCP Ports and UDP Ports.</p> <p>TCP/UDP Service record labels: <b>Port(s) + Protocol</b></p>
<b>Description</b>	All	Text	<p>Service description.</p> <p>TCP/UDP Service record label: Comments</p>
<b>Enabled</b>	TCP* SSL*	<p><b>t</b> = enabled <b>f</b> = disabled Do not use uppercase 'T' or 'F'</p>	<p>Disable the Service globally; or enable, subject to policy</p>
<b>Show in Column</b>	TCP*	<p><b>t</b> = enabled <b>f</b> = disabled Do not use uppercase 'T' or 'F'</p>	<p>Access page display mode</p>
<b>Application Protocol</b>	TCP*	<p><b>ICA</b> <b>RDP</b> <b>VNC</b></p>	<p>Service application protocol. In contrast to the GUI: Disabled, Console, and Web Portal are not used here.</p> <p>A Web Portal is specified by the presence of an address in the Web Portal Launch URL field.</p>
<b>Web Portal Launch URL</b>	TCP: Web	<p>Mapped URL - Use the following form: <b>http[s]://&lt;Local IP&gt;:&lt;First Port&gt;/[path, if any]</b></p> <ul style="list-style-type: none"> <li>The target address is specified by the Device using the Portal</li> <li>A target DNS address for the portal can be identified by the Host Header (and Aliases, if applicable)</li> </ul>	

<b>Launch Path</b>	App*	Path	Location of the remote application that is used in application publishing. Applicable only to targets running Microsoft Terminal Services.
<b>Client Application</b>	TCP	Path	Location of the local application that is launched when the service is initiated.
<b>Host Header</b>	TCP: Web	FQDN	Specify the FQDN of the target website in this field. Per HTTP 1.1, if the Web Portal resides on a single IP address which hosts several websites (such as Apache NameVirtualHost or IIS Host Header Access), this setting is used to identify the correct website target. <b>Note:</b> If Web Portal Launch URL is empty, this field does not populate.
<b>Aliases</b>	TCP: Web	text	If the target web portal is referred to by several different names, enter those names here. Example: If Host Header contains " <a href="http://www.example.com">www.example.com</a> ", while some links on that portal page point to " <a href="http://example.com">example.com</a> " and " <a href="http://someserver.example.com">someserver.example.com</a> ", enter " <a href="http://example.com">example.com</a> " and " <a href="http://someserver.example.com">someserver.example.com</a> " here (without quotes, separated by space or comma) so that requests to that site is handled successfully. <b>Note:</b> If Web Portal Launch URL is empty, this field does not populate.
<b>Hide Web Portal</b>	TCP: Web	t = enabled f = disabled Do not use uppercase 'T' or 'F'	If this portal is not intended to be user-facing - for example, for a graphics file server - select this checkbox so as not to display an access link for the user on the Access page. TCP/UDP Service record: Hide From User

## Messages and Log Formats

This content in this section describes Privileged Access Manager messages that are used in log entries, real-time UI warnings, and other informational output.

**NOTE**

The preformatted messages that are identified here are included in most syslog output (MSG field). Not every message is used in a syslog emission, and not all syslog emissions include a message. For example, some messages are used solely for user interaction. See Syslog Message Formats for more information.

**Message Code List Available from Server**

Use the `getErrorCodes` CLI command to produce a complete list of Credential Manager error codes. The command takes no parameters, and returns an XML structure listing each error code and its description.

For improved readability of the output, we recommend that you direct the XML structure to a separate file, and open it with an XML editor.

**Example**

This example directs the output of the `getErrorCodes` CLI command to a file called `error_codes.xml`.

To retrieve a complete list of Credential Manager error codes:

1. Use the following command: `capam_command -u admin -p password capam=mycompany.com cmdName=getErrorCodes > error_codes.xml` Where *password* is the password of the admin account. Credential Manager returns an XML command string to the `error_codes.xml` file.
2. Open the `error_codes.xml` file with an XML editor, such as Notepad++.

**TIP**

Use the table of contents to access the topics in this section.

**Syslog Message Formats**

Privileged Access Manager has two major formats for Syslog messages, and a few minor ones. The Application field denotes the major component source of the log message.

From 4.0.2 onwards, Privileged Access Manager administrators can standardize Credential Manager Syslog output to Space Delimited instead of XML, and the option to standardize to the JSON format in 4.1.5 and onwards. As a PAM admin, you can standardize syslog audit and metric logs, irrespective of the log.

The default is XML, but you can also use Space Delimited or JSON. For more information, see [Configure a Remote Syslog Server](#), [Configure a Server Control User Activity Server](#), and [Syslog Message Formats](#).

**IMPORTANT**

**IMPORTANT UPDATES to LOGS:** Releases after 4.0.2 implement the following changes for XML attribute tags where duplication was found, as shown in the following table. These updates impact the audit log and the returned data for some CLI commands. To support both backwards compatibility and the new Space Delimited or JSON formats, PAM returns both old and new tags in the audit log and in the CLI returned data for the affected classes.

Class Name	Old Attribute Tag	New Attribute Tag
Agent <c.cw.m.ag>	<ac> = Ack	<ack> = Ack
Patch <c.cw.m.pa>	<ac> = Activated	<avd> = Activated
Authorization <c.cw.m.sa>	<ta.id> = Target.Alias.ID	<al.id> = Target.Alias.ID
Compound.Server <c.cw.m.cs>	<ta.id> = Target.Account.ID	<ac.id> = Target.Account.ID
Password.View.Request.Summary <c.cw.m.pvrs>	<rn> = Requestor.Name	<reqn> = Requestor.Name
Site <c.cw.m.st>	<pr> = Type	<ty> = Type

Event.Base <c.cw.m.evb>	<pi> = Parent.ID	<pri.id> = Parent.ID
-------------------------	------------------	----------------------

**NOTE**

The Message Format you select when you [Configure a Remote Syslog Server](#) **ONLY** applies to the audit and metric logs.

This section describes the formats of these different Syslog messages.

**Session Management Log Formats****Format**

`<PRIORITY>APPLICATION[PID]: MSG`

**PRIORITY** is produced by a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. For example, 13 is "user-level" facility and "Notice" severity. See [Syslog Priority Facility Severity Grid](#) for more information.

**APPLICATION** denotes the major component source of the log message. For Session Management (formerly known as GateKeeper), this value is **gkpsyslog**.

**PID** is the process ID associated with the logged activity, which can help group log messages.

**MSG** includes 12 fields common to Session Logs in the product UI, separated by commas, except after Date/Time.

**MSG Fields**

- **Date/Time:** This field is not labeled, but sent as "created = yyyy-mm-dd hh:mm:ss" (The date and time are sent in UTC.) Example: *created = 2017-11-14 19:55:22*
- **Private IP:** "Private Address" in the UI; if none, a space is logged
- **Public IP:** "Public Address" in the UI; if none, a space is logged
- **Nat/Proxy IP:** "Nat/Proxy Address" in the UI; if none, a space is logged
- **User:** "User Name" in the UI; should not be empty
- **Transaction:** should not be empty
- **Address:** if none, *space, dash, space, dash* is logged; for example: *Address: - -*,
- **Device Name:** if none, *space, dash, space, dash* is logged; for example: *Device Name: - -*,
- **User Group:** if none, *space, dash, dash* is logged; for example: *User Group: --*,
- **Port:** if none, *space, dash, space, dash* is logged; for example: *Port: - -*,
- **Access/Protocol:** "Applet" in the UI; if none, *space, dash, space, dash* is logged; for example: *Access/Protocol: - -*,
- **Service/App:** "Service" in the UI; if none, *space, dash, space, dash* is logged; for example: *Service/App: - -*,
- **Details:** The log messages that are included in the Details field are listed in the [Messages and Log Formats](#) section. This field should not be empty.

Each Session Management Syslog message ends in hex code 0A.

**Examples****Log Records Viewed**

```
<13>gkpsyslog[14289]: created = 2017-11-14 19:55:22 Private IP: , Public IP: , Nat/Proxy
IP: , User: super, Transaction: admin,
Address: - -, Device Name: - -, User Group: --, Port: - -, Access/Protocol: - -,
Service/App: - -,
Details: PAM-CMN-1371: Log records viewed
```

**Session Recording Reconciliation**



```
<28>gkpsyslog[355]: created = 2017-11-14 18:17:03 Private IP: , Public IP: , Nat/Proxy
IP: , User: sessionReconciliation,
Transaction: system, Address: - -, Device Name: - -, User Group: --, Port: - -, Access/
Protocol: - -,
Service/App: - -, Details: PAM-CMN-1989: Ending session recording reconciliation.
0 session recording rows added to table. 0 sidecar(.inf) files added to share.
0 nearly empty files deleted from share.
```

### Super logged in

```
<85>gkpsyslog[9632]: created = 2017-11-14 20:17:06 Private IP: , Public IP: , Nat/Proxy
IP: 130.200.78.105, User: super,
Transaction: login, Address: - -, Device Name: - -, User Group: --, Port: - -, Access/
Protocol: - -,
Service/App: - -, Details: PAM-CMN-0917: User super logged in successfully via local
authentication.
```

## Credential Management Log Formats

### Format

```
<PRIORITY>VERSION
TIMESTAMP
HOSTNAME
APPLICATION
MSG
```

**Priority** is produced by a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. For example, 134 is "local0" facility and "Info" severity. See [Syslog Priority Facility Severity Grid](#) for more information.

**Version** is the version number of the Syslog protocol standard. Currently, the only valid value is "1".

**Timestamp** uses the IETF RFC5424 format including date, time, and time zone. In practice, it is always UTC. For example: 2017-11-12T19:08:18+00:00

**Hostname** is the host name of the originating Privileged Access Manager instance.

**Application** denotes the major component source of the log message. For Credential Management, this value is **pam**.

**MSG** includes either Metric Data or Audit Data.

### Metric Data

Metric log entries result from functions that must be recorded as successes or failures, such as login attempts and password changes.

Each metric log entry contains an object that has several built-in fields. These fields are applied as tag names, and usually have object-specific extended attributes. For example, target accounts use extended attributes to store information that depends on the type of account. Fields are used to store information common to all target accounts. Extended attributes are stored within a tag with attribute ("k") and value ("v") pairs.

The following fields appear in Metric log entries:

- **type:** This field describes type of metric, such as login, or password change. The metric type determines the contents of the description field.
- **level:** This field is not used, and is always set to "1".
- **errorCode:** If the operation failed, the error code identifying the reason for the failure is identified here. A value of "0" denotes success.
- **adminUserId:** This field identifies the user (not necessarily an administrator) that performed the activity in question.
- **Success:** This field identifies whether the operation was successful. If not, the errorCode field identifies why.
- **description:** This field contains an embedded field (typically a hashmap) representing details specific to the type of metric.

Credential Management metric log entries appear as strings, but can be reformatted to display their structure.

The following code provides a sample in XML format. For a space-delimited example, see [Metric Detail Space-Delimited Example](#). For a JSON formatted example, see [Metric Detail JSON Example](#).

```
<Metric>
  <type>viewAccountPassword</type>
  <level>1</level>
  <description>
    <hashmap>
      <k>commandInitiator</k><v>USER</v>
      <k>adminUserID</k><v>super</v>
      <k>reason</k><v></v>
      <k>selectedComponent</k><v>0</v>
      <k>Attribute.descriptor2</k><v></v>
      <k>Attribute.descriptor1</k><v></v>
      <k>TargetAccount.ID</k><v>1005</v>
      <k>TargetApplication.name</k><v>SQLServer</v>
      <k>reasonDetails</k><v></v>
      <k>password</k><v></v>
      <k>TargetServer.hostName</k><v>100.130.156.40</v>
      <k>TargetAccount.accessType</k><v></v>
      <k>referenceCode</k><v></v>
      <k>adminPassword</k><v></v>
      <k>TargetAccount.userName</k><v>xmd_user</v>
    </hashmap>
  </description>
  <errorCode>0</errorCode>
  <userID>super</userID>
  <success>true</success>
  <originatingIPAddress></originatingIPAddress>
  <originatingHostName></originatingHostName>
  <extensionType></extensionType>
</Metric>
```

### ***Metric Detail Space-Delimited Example***

```
05-25-2023 13:38:40 Local0.Warning 1.2.3.4 1 2023-01-25T19:38:39+00:00 PAM-Node1 pam - metric DETAIL |
type=viewAccountPassword level=1 description=hashmap { [ commandInitiator=USER ] [ adminUserID=super ]
[ reason=Other ] [ Attribute.descriptor2= ] [ Attribute.descriptor1= ] [ reasonDetails=One-click access
```

```
required ] [ password= ] [ TargetAccount.accessType= ] [ connectionTimeout=0 ] [ adminPassword= ]
[ selectedComponent=0 ] [ Attribute.awsAccessKeyAlias= ] [ PasswordViewRequest.comments= ]
[ TargetAccount.ID=74001 ] [ TargetApplication.name=Test_TargetApplication ] [ TargetServer.hostName=Test ]
[ referenceCode= ] [ PasswordViewRequest.requestPeriodStart=2023-01-25 19:38:00 ]
[ PasswordViewRequest.requestPeriodEnd=2023-01-25 20:38:00 ] [ TargetAccount.userName=Test_TargetAccount ] }
errorCode=4625 userID=super success=false originatingIPAddress= originatingHostName= extensionType=
```

### Metric Detail JSON Example

```
Sep 7 10:04:00 10.252.45.109 1 2023-09-07T14:05:53+00:00 PAM-Node1 pam - audit DETAIL {"TargetAccount":
{"LastVerified":1694095553653,"PasswordViewPolicy":1000,"UserName":"super","CacheAllow":true,"ServerKeyID":1001,"Unmana
{"isProvisionedAccount":false,"protocol":"SSH2
_PASSWORD_AUTH","verifyThroughOtherAccount":false,"discoveryGlobal":false,"discoveryAllowed":false,"extensionType":"un
```

### Audit Log Entries

Credential Management audit log entries appear as strings, but can be reformatted to display their structure.

The following code provides a sample in XML format. For a space-delimited example, see [Audit Detail Space-Delimited Example](#). For a JSON example, see [Audit Detail JSON Example](#).

```
<c.cw.m.ts>
  <bm.id>1004</bm.id>
  <bm.cd>1473152059000</bm.cd>
  <bm.cu>super</bm.cu>
  <bm.ud>1473234607186</bm.ud>
  <bm.uu>super</bm.uu>
  <bm.ha>FUwULFPtQlT4...f+AwUW4Ha8k=</bm.ha>
  <bm.at.li>
    <c.cw.m.at>
      <bm.id>1004</bm.id>
      <bm.cd>1473152059000</bm.cd>
      <bm.cu>super</bm.cu>
      <bm.ud>1473152881000</bm.ud>
      <bm.uu>super</bm.uu>
      <bm.ha>Wpkmh+aP0lrWk/...8s57Mjowo=</bm.ha>
      <at.na>descriptor1</at.na>
      <at.ob.id>1004</at.ob.id>
      <at.ob.cl>c.cw.m.ts</at.ob.cl>
    </c.cw.m.at>
    <c.cw.m.at>
      <bm.id>1005</bm.id>
      <bm.cd>1473152059000</bm.cd>
      <bm.cu>super</bm.cu>
      <bm.ud>1473152881000</bm.ud>
      <bm.uu>super</bm.uu>
      <bm.ha>Wpkmh+aP0lrWk/A...s57Mjowo=</bm.ha>
      <at.na>descriptor2</at.na>
      <at.ob.id>1004</at.ob.id>
      <at.ob.cl>c.cw.m.ts</at.ob.cl>
    </c.cw.m.at>
  </bm.at.li>
```

```

    <hn>123.123.123.000</hn>
    <ip>123.123.124.000</ip>
    <dn>redhat</dn>
</c.cw.m.ts>

```

These log entries are wrapped by <c.cw.m...> tags.

- c.cw.m = com.cloakware.model.

#### NOTE

"Cloakware" is an internal name for the Credential Management function.

- bm = BaseModel is the parent of all object types. This tag is found in all objects for their common attributes.
- id = identification number for this object
  - For example, "id" may be a target account ID, a target server ID, or a Password View Request ID.
  - The name of a target account may change but its ID does not.
  - Metric log entries only specify the ID, but not the name. The session log entries are comprehensive, so you can find an ID when given the name.

Class IDs begin with c.cw.m. The fourth element identifies the object. The elements specific to that object follow each object code.

```

ac = Account
    ca = cache allowed
    cd = cache duration
    pv = password verified
    um = unmanaged
    un = User Name
    uoid = owner user
ID
ach = Account History
    act = Account
    ht = Historical
Tag
fl = Filter
    an = object
    ex = expression
    ty =
operator
gr = Group (Target or Requestor)
    ty = type
    dy = dynamic
    gro = read-only
    pe = Request Server
ID
po = Password Composition Policy

pvp = Password View Policy
    cpov = Change Password On View
    cpoconnend = Change Password On Connection End
    cposessend = Change Password On Session End

```

---

cposso = Change Password On SSO  
pci = Password Change Interval  
cico = Check-out Check-in Required  
cci = Check-out Check-in Interval  
da =Dual Authorization  
ai =Dual Approval Interval  
mi =Max Interval  
md =Max Days  
rr = Reason Required  
rrsso = Reason Required SSO  
en =Email Notification  
enda = Email Notification for Dual Approvers  
enau =Email Only Active Users  
ro = Read

Only

pvr = Password View Request  
ar = Approval  
rc = Reason Code  
re =

Reason

ro = Role

rs = Request server  
atr = action required  
av = Active  
ty =

type

sa = A2A  
ce = Check Execution User  
cf = Check File Path  
cp = Check Path  
cs = Check Script Hash  
eu = Execution

User

sc = Script

sj = Scheduled Job

sysp = System Properties  
pn = property name  
pv = property  
value

ta = Target Alias

tp = Target Application

ts = Target Server

ug = User Group

us = User  
 fn = First Name  
 ln = Last Name  
 st = Status  
 em =  
 Email

The following elements are common to multiple classes:

ad = Approval Description  
 cd = created date, in UNIX time, with milliseconds  
 cu = Creating User  
 de = Description  
 dn = Device name  
 ha = hash  
 hn = Host name  
 ip = IP Address  
 na = Attribute name  
 phn = preserve host name  
 po = port  
 ps = patch status  
 rg = Request Group  
 sid = Site ID  
 skid = server key ID  
 sp = System property  
 ta = Target application ID  
 tg = Target Group  
 ud = updated date, in UNIX time, with milliseconds  
 uu = Updating User  
 va = Attribute Value

### **Audit Detail Space-Delimited Example**

```
05-25-2023 13:39:07 Local0.Info 1.2.3.4 1 2023-01-25T19:39:07+00:00 PAM-Node1 pam - audit DETAIL
Target.Account | ID=78001 Create.Date=1650645399000 Create.User=super Update.Date=1674675547003
Update.User=super Hash=N6wSqfUT3odsafs4Ferxi8mU= Attribute.List={ [ ID=1615001 Create.Date=1674675547005
Create.User=super Update.Date=1674675547005 Update.User=super Attribute.Name=isProvisionedAccount
Attribute.Value=false Attribute.Object.ID=78001 Attribute.Object.Class.ID=c.cw.m.ac ] [ ID=0
Create.Date=0 Update.Date=0 Attribute.Name=otherAccount Attribute.Object.ID=0 ] [ ID=0 Create.Date=0
Update.Date=0 Attribute.Name=descriptor2 Attribute.Object.ID=0 ] [ ID=0 Create.Date=0 Update.Date=0
Attribute.Name=discoveryGlobal Attribute.Value=false Attribute.Object.ID=0 ] [ ID=0 Create.Date=0
Update.Date=0 Attribute.Name=descriptor1 Attribute.Object.ID=0 ] [ ID=0 Create.Date=0 Update.Date=0
Attribute.Name=extensionType Attribute.Value=mssql Attribute.Object.ID=0 ] [ ID=0 Create.Date=0 Update.Date=0
Attribute.Name=discoveryAllowed Attribute.Value=false Attribute.Object.ID=0 ] [ ID=0 Create.Date=0
Update.Date=0 Attribute.Name=useOtherAccountToChangePassword Attribute.Value=false Attribute.Object.ID=0 ] }
Target.Application.ID=33001 User.Name=test1_account1 Cache.Duration=30 Cache.Allow=true Cache.Behavior=1
Unmanaged=true Account.Synchronized=false Password.Verified=false Compound.Account=false Server.Key.ID=1001
Owner.User.ID=-1 Last.Used=1651687071000 Password.View.Policy=1000
```

## Audit Detail JSON Example

```
Sep 7 10:04:00 10.252.45.109 1 2023-09-07T14:05:53+00:00 PAM-Node1 pam - audit DETAIL {"TargetAccount":
{"LastVerified":1694095553653,"PasswordViewPolicy":1000,"UserName":"super","CacheAllow":true,"ServerKeyID":1001,"Unmana
{"isProvisionedAccount":false,"protocol":"SSH2
_PASSWORD_AUTH","verifyThroughOtherAccount":false,"discoveryGlobal":false,"discoveryAllowed":false,"extensionType":"un
```

## GKMonitor

### Format

```
<PRIORITY>APPLICATION[PID]: MSG
```

**PRIORITY** is produced by a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. For example, 85 is “security/auth” facility and “Notice” severity. See [Syslog Priority Facility Severity Grid](#) for more information.

**APPLICATION** denotes the major component source of the log message. For these messages, this value is `gkmonitor`.

**PID** is the process ID associated with the logged activity, which can help group log messages.

**MSG** includes only a simple log message. The date and time are not sent.

### Example

#### User account disabled

```
<85>gkmonitor[12371]: PAM-CMN-2135="Disabled user account: {0} removed from PAM
```

## Logwatch

### Format

```
<PRIORITY>APPLICATION[PID]: MSG
```

**PRIORITY** is produced by a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. For example, 28 is “system” facility and “Warning” severity. See [Syslog Priority Facility Severity Grid](#) for more information.

**APPLICATION** denotes the major component source of the log message. For these messages, this value is `logwatch`.

**PID** is the process ID associated with the logged activity, which can help group log messages.

**MSG** includes only a simple log message. The date and time are not sent.

### Example

#### Starting up logwatch

```
<28>logwatch[1]: Starting up logwatch
```

## Other Messages

### Format

```
<PRIORITY>VERSION
TIMESTAMP
HOSTNAME
MSG
```

**PRIORITY** is produced by a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. For example, 134 is "local0" facility and "Info" severity. See [Syslog Priority Facility Severity Grid](#) for more information.

**VERSION** is the version number of the Syslog protocol standard. Currently, the only valid value is "1".

**TIMESTAMP** does not conform to IETF specifications. The year and time zone are not included, and the month is an English abbreviation. In practice, it is always UTC. **For example:** Sep 18 22:09:54

**HOSTNAME** is the hostname of the originating Privileged Access Manager instance.

**MSG** entries are tagged as <Metric> or formatted like Audit entries, but not labeled as such. The audit-type entries are typically paired with a Metric entry.

### Examples

#### System Startup

```
<134>1 Sep 18 20:09:25 uslipam13-133 <Metric>systemStartup 1 0 system true 130.200.13.133 uslipam13-133</Metric>
```

#### Register Request Server 1

```
<134>1 Sep 12 22:09:31 uslipam13-133
<Metric>
  <type>registerRequestServer</type>
  <level>1</level>
  <description>
    <hashmap>
      <k>commandInitiator</k><v>USER</v>
      <k>enablefips</k><v>true</v>
      <k>version</k><v>4.13.0</v>
      <k>RequestServer.ID</k><v>1000</v>
      <k>commandName</k><v>clientLogin</v>
      <k>port</k><v>27077</v>
      <k>osarch</k><v>x86</v>
      <k>osversion</k><v>6.1</v>
      <k>nodeid</k>
      <v>&lt;?xml version="1.0" encoding="utf-8" ?&gt;&lt;nodeid&gt;&lt;macaddr&gt;
00:50:56:86:0E:4F&lt;/macaddr&gt;&lt;machineid&gt;
4_39ec5d8a_0_0-Intel-PIIX4_Internal_IDE_Channel&lt;/machineid&gt;
&lt;applicationtype&gt;cspm_agent&lt;/applicationtype&gt;&lt;/nodeid&gt;</v>
      <k>osname</k><v>Windows 7</v>
    </hashmap>
  </description>
  <errorCode>0</errorCode>
  <userID>client</userID>
  <success>true</success>
  <originatingIPAddress>10.130.236.131</originatingIPAddress>
  <originatingHostName>10.130.236.131</originatingHostName>
  <extensionType></extensionType>
</Metric>
```

#### Register Request Server 2



```

<134>1 Sep 12 22:09:31 uslipam13-133
<c.cw.m.rs>
  <bm.id>1000</bm.id>
  <bm.cd>1505255190000</bm.cd>
  <bm.cu>client</bm.cu>
  <bm.ud>1505255191851</bm.ud>
  <bm.uu>client</bm.uu>
  <bm.ha>P2yCGNvoSpvZiEmtLwohN7kXa5w=</bm.ha>
  <ty>AGENT</ty>
  <hn>10.130.236.131</hn>
  <ip>10.130.236.131</ip>
  <dn>10.130.236.131</dn>
  <po>27077</po>
  <nk>{1}ada8fd1fdccb2a...3587101e2330685f7e</nk>
  <ac>>false</ac>
  <av>>false</av>
  <atr>>true</atr>
  <at>102</at>
  <cf>NgdtGgAjjF7QHPap9Kqd2mpSS1M=</cf>
  <on>Windows 7</on>
  <ov>6.1</ov>
  <oa>x86</oa>
  <ct>java</ct>
  <sid>1000</sid>
  <phn>>false</phn>
  <skid>1</skid>
  <pl>win</pl>
  <ps>Disabled</ps>
  <cvn>4.13.0</cvn>
  <cfid>1505255190000</cfid>
  <cst>2</cst>
  <csudt>1505255189000</csudt>
</c.cw.m.rs>

```

## Syslog Priority Facility Severity Grid

The Priority value that Privileged Access Manager sends to Syslog servers is derived from a standard IETF syslog grid of Facility by Severity. Syslog servers might extrapolate the Facility and Severity values. Find the value, from 0 to 191, in the grid, and see the column and row values. For example, a Priority value of 13 is “user-level” Facility and “Notice” Severity.

	Severity	Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
Facility		0	1	2	3	4	5	6	7
kernel	0	0	1	2	3	4	5	6	7
user-level	1	8	9	10	11	12	13	14	15
mail	2	16	17	18	19	20	21	22	23
system	3	24	25	26	27	28	29	30	31

secur/auth	4	32	33	34	35	36	37	38	39
syslog	5	40	41	42	43	44	45	46	47
lpd/printer	6	48	49	50	51	52	53	54	55
news/nntp	7	56	57	58	59	60	61	62	63
uucp	8	64	65	66	67	68	69	70	71
time	9	72	73	74	75	76	77	78	79
secur/auth	10	80	81	82	83	84	85	86	87
ftp	11	88	89	90	91	92	93	94	95
nntp	12	96	97	98	99	100	101	102	103
logaudit	13	104	105	106	107	108	109	110	111
logalert	14	112	113	114	115	116	117	118	119
clock	15	120	121	122	123	124	125	126	127
local0	16	128	129	130	131	132	133	134	135
local1	17	136	137	138	139	140	141	142	143
local2	18	144	145	146	147	148	149	150	151
local3	19	152	153	154	155	156	157	158	159
local4	20	160	161	162	163	164	165	166	167
local5	21	168	169	170	171	172	173	174	175
local6	22	176	177	178	179	180	181	182	183
local7	23	184	185	186	187	188	189	190	191

## PAM-AGT: CA PAM Access Agent Messages

PAM-AGT-1000: This version of PAM is not supported by the Agent. Please connect to another PAM server.

PAM-AGT-1001: CA PAM Agent Service is not started. Please start this service before continuing.

PAM-AGT-1002: Cannot connect to the PAM server at this address. Please re-check your server name/IP, and ensure your PAM instance is running.

PAM-AGT-1003: This service has already been activated.

PAM-AGT-1004: A Password View Request for this Credential is already pending.

PAM-AGT-1005: Reason is required, please select one

PAM-AGT-1006: Error importing certificate. Please check your certificate and try again.

PAM-AGT-1007: Error exporting certificate.

PAM-AGT-1008: Error removing the certificate

PAM-AGT-1009: Host and Port values are required for this proxy mode.

PAM-AGT-1010: Proxy URL is required for this proxy mode.

PAM-AGT-1011: Cannot activate this service. Another service with the same device and local port(s) has already been activated.

PAM-AGT-1012: Error occurred during authentication.

PAM-AGT-1013: Error launching installer. If this problem persists, please contact support.

PAM-AGT-1013: Dual authorization for this credential is still pending. Try again after approval.

PAM-AGT-1014: Dual authorization for this credential has been denied.

PAM-AGT-1100: Service activation failed. Please restart the PAM Agent and the PAM Agent service and try again.

PAM-AGT-1101: Error setting up Agent services. Please restart the PAM Agent and the PAM Agent service and try again.

## PAM-CF: Connector Framework Messages

PAM-CF-0001 = The Custom Connector server is inaccessible or its configuration is invalid.

PAM-CF-0002 = There is an error on the Custom Connector server.

PAM-CF-0005 = Failed to validate target connector attributes. {0}

PAM-CF-0006 = Invalid connector framework configuration parameters : {0}

PAM-CF-0007 = Connector Framework Certificate is expiring in less than {0} day(s).

PAM-CF-0008 = Connector Framework Certificate has expired.

## PAM-CLNT: PAM Client Messages

PAM-CLNT-0000 = Application error occurred in RDP client: {0}

PAM-CLNT-0001 = Wrong Web SSO configuration.

PAM-CLNT-0002 = Incorrect login URL.

PAM-CLNT-0003 = Unknown Web SSO status: {0}

PAM-CLNT-0004 = Auto login inner error. Reason: {0}

PAM-CLNT-0005 = Auto login timeout expired, possibly due to wrong credentials.

PAM-CLNT-0006 = SSO credentials are invalid.

PAM-CLNT-0007 = Session disconnected due to a problem with session recording.

PAM-CLNT-0008 = Session can't be established due to a problem with session recording

PAM-CLNT-0009 = Local folder has been created by user {0}

PAM-CLNT-0010 = Local file has been created by user {0}

PAM-CLNT-0011 = Remote folder has been created by user {0}

PAM-CLNT-0012 = Remote file has been created by user {0}

PAM-CLNT-0013 = Local folder has been renamed to {0} by user {1}

PAM-CLNT-0014 = Local file has been renamed to {0} by user {1}

PAM-CLNT-0015 = Remote folder has been renamed to {0} by user {1}

PAM-CLNT-0016 = Remote file has been renamed to {0} by user {1}

PAM-CLNT-0017 = Local folder has been deleted by user {0}

PAM-CLNT-0018 = Local file has been deleted by user {0}

PAM-CLNT-0019 = Remote folder has been deleted by user {0}

PAM-CLNT-0020 = Remote file has been deleted by user {0}

PAM-CLNT-0021 = Uploaded {0} to {1} as user {2}

PAM-CLNT-0022 = Downloaded {0} from {1} as user {2}

PAM-CLNT-0023 = Executed '{0}' using transparent login as {1}

PAM-CLNT-0024 = A connection from {0} to service '{1}' was attempted by an unauthorized session '{2}' on '{3}'PAM-CLNT-0025="{0}"

## PAM-CM: Credential Manager Messages

The following messages are created by Credential Manager. Certain messages are grouped by subheading.

PAM-CM-0000 = Downloaded Certificate {0}

PAM-CM-0001 = Downloaded CSR {0}

PAM-CM-0002 = Downloaded private key file {0}

PAM-CM-0004 = Downloaded database file {0}

PAM-CM-0005 = User tried and failed to upload a database or configuration file with invalid characters in the file name and / or an improper file extension.

PAM-CM-0006 = Config file {0} uploaded successfully

PAM-CM-0007 = Database file {0} uploaded successfully

PAM-CM-0008 = Run ping on host {0}.

PAM-CM-0009 = Run traceroute on host {0}.

PAM-CM-0010 = Run Port Scan on IP address: {0}. Ports: {1}.

PAM-CM-0011 = Run nslookup on host {0}.

PAM-CM-0012 = {0} export completed.

PAM-CM-0013 = {0} import completed.

PAM-CM-0014 = Uploaded license file {0}

PAM-CM-0015 = Downloaded log file {0}.

PAM-CM-0016 = File {0} uploaded successfully. For this change to take effect, please restart Tomcat.

PAM-CM-0018 = File {0} uploaded successfully! Please delete the Node Secret file if it exists to clear old cache.

PAM-CM-0019 = Job {0} deleted.

PAM-CM-0020 = Job {0} cancelled.

PAM-CM-0021 = Unable to load PAM certificate for SSO user {0}. User will not be able to log-in

PAM-CM-0022 = Account Scan Profile {0} created.

PAM-CM-0023 = Account Scan Profile {0} deleted.

PAM-CM-0024 = Account Scan Profile {0} updated.

PAM-CM-0025 = Config exception: {0}

PAM-CM-0026 = Error creating object: {0}

PAM-CM-0027 = CA Single Sign-On Web Agent disabled. For this change to take effect, please restart Apache.

PAM-CM-0028 = Restarting Apache Web Server

PAM-CM-0029 = Configuration of CA Single Sign-On Web Agent complete. For this change to take effect, please restart Apache.

PAM-CM-0030 = Registration failed ('{0}');

PAM-CM-0032 = CA Single Sign-On Web Agent registration failed. Host config object not found.

PAM-CM-0033 = CA Single Sign-On Web Agent registration failed. Invalid credentials.

PAM-CM-0034 = CA Single Sign-On Web Agent registration failed. Unknown administrator.

PAM-CM-0035 = Object empty: {0}

PAM-CM-0036 = Updated system certificate to {0}

PAM-CM-0037 = Problem updating system certification {0}

PAM-CM-0038 = Problem updating system certification

PAM-CM-0039 = Unable to perform the operation. Please contact System Administrator.

PAM-CM-0040 = Created Self-Signed Certificate {0}

PAM-CM-0041 = Created CSR {0}

PAM-CM-0042 = There is invalid CRL URL format: {0}

PAM-CM-0043 = There is invalid CRL file: {0}

PAM-CM-0044 = CRL file: {0} was added.

PAM-CM-0045 = Disabling SAML IdP component

PAM-CM-0046 = SAML IdP is already disabled

PAM-CM-0047 = Restarting after SAML IdP change

PAM-CM-0048 = SAML IdP is already enabled

PAM-CM-0049 = Enabling SAML IdP component

PAM-CM-0050 = CA PAM SAML Identity Provider configuration updating: Entity ID = {0}, FQDN = {1}, Certificate = {2}

PAM-CM-0051 = The CA PAM database has been compacted successfully

PAM-CM-0052 = Reset CA PAM database failed: {0}

PAM-CM-0053 = Database backup schedule saved successfully

PAM-CM-0054 = Database backup schedule deleted successfully

PAM-CM-0055 = Mount unsuccessful. Please contact administrator.

PAM-CM-0056 = NFS mount operation unsuccessful. Mount point: {0} Hostname: {1}

PAM-CM-0057 = NFS mounting performed successfully. Mount point: {0} Hostname: {1}

PAM-CM-0058 = CIFS mount operation unsuccessful. Mount point: {0} Hostname: {1}  
PAM-CM-0059 = CIFS mounting performed successfully. Mount point: {0} Hostname: {1}  
PAM-CM-0060 = Mount unsuccessful. Please contact administrator. Not existent S3 bucket {0}  
PAM-CM-0061 = Mount unsuccessful. Please contact administrator {0}  
PAM-CM-0062 = S3 mounting performed successfully  
PAM-CM-0063 = The CA PAM database has been reset successfully  
PAM-CM-0064 = CA PAM configuration restored successfully from file {0}. CA PAM is being rebooted.  
PAM-CM-0065 = Could not restore CA PAM configuration: {0}  
PAM-CM-0066 = Could not restore the database because disk is over half full.  
PAM-CM-0067 = CA PAM database restored successfully from file {0}. CA PAM is being rebooted.  
PAM-CM-0068 = Could not restore the database: {0}. Contact your CA PAM administrator.  
PAM-CM-0069 = Unable to save the database to a file: {0}  
PAM-CM-0070 = Unable to save CA PAM configuration to a file: {0}  
PAM-CM-0071 = {0} CA PAM configuration saved successfully to {1}  
PAM-CM-0073 = Database file {0} deleted successfully.  
PAM-CM-0074 = Unable to delete database file {0}: File not found.  
PAM-CM-0075 = Unable to delete database file {0}: {1}.  
PAM-CM-0076 = Unmounting performed successfully  
PAM-CM-0077 = Unmount operation unsuccessful.  
PAM-CM-0078 = Account {0} managed.  
PAM-CM-0081 = Device {0} managed.  
PAM-CM-0082 = Session recording '{0}' was viewed  
PAM-CM-0083 = Monitor started successfully  
PAM-CM-0084 = Monitor stopped successfully  
PAM-CM-0085 = Updated monitoring configuration. Admin email: {0}., SMTP Server: {1}., From Address: {2}.  
PAM-CM-0086 = Problem updating the configuration: {0}  
PAM-CM-0087 = Changed Monitor startup flag to on.  
PAM-CM-0088 = Changed Monitor startup flag to off.  
PAM-CM-0089 = Added new route: Destination: {0} Netmask: {1} Gateway: {2} Device: {3} Metric: {4}  
PAM-CM-0090 = Added new route: Destination: {0} Gateway: {1} Device: {2}  
PAM-CM-0091 = Deleted route: Destination: {0} Netmask: {1} Gateway: {2} Device: {3} Metric: {4}  
PAM-CM-0092 = Deleted route: Destination: {0} Gateway: {1} Device: {2}  
PAM-CM-0093 = Successfully restarted networking  
PAM-CM-0094 = Network Interface: {0} disabled.  
PAM-CM-0095 = Network Interface: {0} Speed: {1}, Duplex: {2}, IP address: {3}, Netmask: {4}, Broadcast: {5}, IPv6 Address: {6}.  
PAM-CM-0096 = Network settings updated successfully . Hostname: {0}, Domain Name: {1}, Default Gateway: {2}, DNS Servers: {3}  
PAM-CM-0097 = Device Scan Profile {0} created.  
PAM-CM-0098 = Device Scan Profile {0} deleted.  
PAM-CM-0099 = Device Scan Profile {0} updated.  
PAM-CM-0100 = Updated Microsoft Office 365 configuration  
PAM-CM-0101 = Cleared Microsoft Office 365 configuration  
PAM-CM-0102 = Office 365 configuration test: Connected successfully to the supplied URLs  
PAM-CM-0103 = Office 365 configuration test: Error connecting to the supplied URLs  
PAM-CM-0104 = The user has acknowledged the warnings related to rebooting an appliance (for activating or deactivating FIPS) while the cluster is running.  
PAM-CM-0105 = Activated FIPS Mode  
PAM-CM-0106 = Deactivated FIPS Mode  
PAM-CM-0107 = The user has acknowledged the warnings related to rebooting an appliance (for activating or deactivating FIPS) while the cluster is running. Activated FIPS Mode  
PAM-CM-0108 = The user has acknowledged the warnings related to rebooting an appliance (for activating or deactivating FIPS) while the cluster is running. Deactivated FIPS Mode

PAM-CM-0109 = The user has acknowledged the warnings related to rebooting an appliance while the cluster is running. The appliance will now be powered off.

PAM-CM-0110 = Powered off the appliance

PAM-CM-0111 = Shutting down...

PAM-CM-0112 = The user has acknowledged the warnings related to rebooting an appliance while the cluster is running. The appliance will now be rebooted.

PAM-CM-0113 = Rebooted the appliance

PAM-CM-0114 = Rebooting...

PAM-CM-0115 = {0} Configuration Updated Successfully! Added server {1}:{2}

PAM-CM-0116 = {0} Configuration Updated Successfully! Deleted server {1}:{2}

PAM-CM-0117 = Object not found: {0}

PAM-CM-0118 = Radius server on {0}: port {1} not found.

PAM-CM-0119 = File {0} deleted successfully. For this change to take effect, please restart Tomcat.

PAM-CM-0120 = File {0} deleted successfully!

PAM-CM-0121 = {0}

PAM-CM-0122 = Connected successfully to the ActiveMQ Console on host {0}

PAM-CM-0123 = Could not connect to the ActiveMQ Console on host {0}

PAM-CM-0124 = Server Control integration module was activated

PAM-CM-0125 = Server Control integration module was deactivated

PAM-CM-0126 = Could not activate Server Control integration module

PAM-CM-0127 = Could not deactivate Server Control integration module

PAM-CM-0128 = Unable to delete {0}

PAM-CM-0129 = {0} deleted successfully

PAM-CM-0130 = Certificate Upload: Unknown Format ({0})

PAM-CM-0131 = Unknown Format

PAM-CM-0132 = An error occurred while setting the cluster tuning mode.

PAM-CM-0133 = Database error

PAM-CM-0134 = Data is being collected. Graphs will begin to be generated within the next twenty minutes.

PAM-CM-0135 = An error occurred setting debug SSHD Mode

PAM-CM-0136 = Created System Diagnostic file

PAM-CM-0137 = The license was not updated. Uploaded license file could not be verified or read.

PAM-CM-0138 = Log file {0} deleted successfully.

PAM-CM-0139 = Unable to delete log file {0}: File not found.

PAM-CM-0140 = Unable to delete log file {0}: {1}.

PAM-CM-0141 = Mount unsuccessful. Please contact administrator

PAM-CM-0142 = All logs have been purged.

PAM-CM-0143 = Unable to purge the logs. Please, contact your administrator.

PAM-CM-0144 = Purged logs up till {0}

PAM-CM-0145 = Changed automatic Log Purge Settings. Status: Enabled, Purge interval: {0}, Email flag: {1}, Email size: {2} MB.

PAM-CM-0146 = Changed automatic Log Purge Settings. Status: Disabled

PAM-CM-0147 = External Log Settings saved successfully.

PAM-CM-0148 = Created new log table on the external server.

PAM-CM-0149 = Created new log\_user\_group table on the external server.

PAM-CM-0150 = Created new log\_device\_group table on the external server.

PAM-CM-0151 = Connection to the database established successfully and tables created.

PAM-CM-0152 = Connection to the database established successfully.

PAM-CM-0153 = Saved logs up till {0}

PAM-CM-0154 = Unable to write the logs to a file! Please, contact your administrator!

PAM-CM-0155 = Updated Syslog Settings. Status: Enabled, Remote Server(s): {0}, with port: {1}

PAM-CM-0156 = Updated Syslog Settings. Status: Disabled

PAM-CM-0157 = Keystroke Logging configuration updated successfully. Syslog: {0}. NFS/CIFS/S3 CLI Recording: {1}. NFS/CIFS/S3 Graphical Recording: {2}.



PAM-CM-0158 = {0}. Settings saved successfully. Mount point: {1}. Hostname: {2}  
PAM-CM-0159 = Updated Session Recording to be Security Safe  
PAM-CM-0160 = Updated Session Recording to be Operationally Safe  
PAM-CM-0161 = You do not have sufficient permissions to perform this operation.  
  
PAM-CM-0162 = Payload id does not match url id: {0} != {1}  
PAM-CM-0163 = Must specify all filter parameters (column, op, value) or none  
PAM-CM-0164 = Invalid Operator filter. Valid values = EQ, NE  
PAM-CM-0165 = Error retrieving object by id: {0}  
PAM-CM-0166 = Error retrieving object by name: {0}  
PAM-CM-0167 = Error updating object: {0}  
PAM-CM-0168 = Call to PAM service controller failed: {0}  
PAM-CM-0169 = Error connecting to the database. Transaction canceled  
PAM-CM-0170 = Transaction error with the database. Transaction canceled  
PAM-CM-0171 = Target Server not found for host: {0}  
PAM-CM-0172 = Number of devices that were successfully managed: {0}  
PAM-CM-0173 = Number of devices that were NOT successfully managed: {0}  
PAM-CM-0174 = Target Application not found: {0}  
PAM-CM-0175 = Target Account {0} already exists. No modifications made.  
PAM-CM-0176 = {0} is not a valid {1} IP Address.  
PAM-CM-0177 = Profile name is not defined.  
PAM-CM-0178 = {0} name {1} already exists.  
PAM-CM-0179 = {0} is not a valid parameter.  
  
PAM-CM-0180 = Radius server on {0}: port {1} already exists.  
PAM-CM-0181 = Splunk server on {0}: port {1} already exists.  
PAM-CM-0182 = Account management failed for account {0} with the following error: {1}  
PAM-CM-0183 = Logo was reverted to original logo.  
PAM-CM-0184 = Logo file {0} was successfully uploaded.  
PAM-CM-0185 = Action was applied for {0} {1}.  
PAM-CM-0186 = Shared Key is not allowed to download  
PAM-CM-0187 = Private Key is not allowed to be downloaded  
PAM-CM-0188 = Required Remedy licensed files could not be found.  
PAM-CM-0189 = {0} is not defined.  
PAM-CM-0190 = Please enter the required password that will be used to encrypt the private key!  
PAM-CM-0191 = Please enter the confirmed password that will be used to encrypt the private key!  
PAM-CM-0192 = The confirmed password does not match the password!  
PAM-CM-0193 = The passphrase contains invalid space or - characters!  
PAM-CM-0194 = Unable to upload file  
PAM-CM-0195 = The key file for the certificate {0} is missing  
PAM-CM-0196 = Could not change {0}  
PAM-CM-0197 = Cannot update CRL configuration: {0}  
PAM-CM-0198 = The IdP settings cannot be updated while the cluster is on  
PAM-CM-0199 = Unknown certificate {0} selected  
PAM-CM-0200 = SAML Metadata file must be an XML file  
PAM-CM-0201 = Verification Error {0}  
PAM-CM-0202 = Invalid Tomcat log level submitted  
PAM-CM-0203 = Tomcat Log Level updated.  
PAM-CM-0204 = Tomcat Log Level could not be updated.  
PAM-CM-0205 = Database updated successfully  
PAM-CM-0206 = Applet Log Level updated.  
PAM-CM-0207 = Applet Log Level could not be updated.  
PAM-CM-0208 = Web service log level updated successfully  
PAM-CM-0209 = Web service log level could not be updated

PAM-CM-0212 = CA PAM As SAML SP Log Level updated  
PAM-CM-0213 = CA PAM As SAML IdP Log Level updated  
PAM-CM-0214 = CA PAM As SAML IdP Log Level could not be updated  
PAM-CM-0216 = An error occurred setting Maintenance Mode  
PAM-CM-0217 = Maintenance mode has been enabled for this appliance  
PAM-CM-0218 = Maintenance mode has been disabled for this appliance  
PAM-CM-0219 = AACTRL debug mode has been enabled for this appliance  
PAM-CM-0220 = AACTRL debug mode has been disabled for this appliance  
PAM-CM-0221 = Remote CA PAM Debugging Services active until {0} UTC  
PAM-CM-0222 = Remote CA PAM Debugging Services turned off  
PAM-CM-0223 = Cluster tuning mode turned on  
PAM-CM-0224 = Cluster tuning mode turned off  
PAM-CM-0228 = External REST API Access has been Enabled  
PAM-CM-0229 = External REST API Access has been Disabled  
PAM-CM-0230 = External Password Authority API Access has been Enabled  
PAM-CM-0231 = External Password Authority API Access has been Disabled  
PAM-CM-0232 = VMware console could not be Enabled  
PAM-CM-0233 = VMware console could not be Disabled  
PAM-CM-0234 = No common name specified  
PAM-CM-0235 = IPv6 is not supported  
PAM-CM-0236 = You entered an invalid value for Subject Alternative Name. Please enter only IP addresses and/or FQDNs  
PAM-CM-0237 = Unknown certificate {0} selected  
PAM-CM-0238 = Invalid Password Entry  
PAM-CM-0239 = Invalid Confirmed Password Entry  
PAM-CM-0240 = Invalid Provider Entry  
PAM-CM-0241 = Confirmed Password Does Not Match The Password  
PAM-CM-0242 = The SAML entity ID for the IdP is required  
PAM-CM-0243 = The fully qualified hostname for the SAML IdP is required  
PAM-CM-0244 = The fully qualified hostname for the SAML IdP is not a valid hostname  
PAM-CM-0245 = Invalid Signature Algorithm Specified! Valid values are: {0}  
PAM-CM-0246 = Applied patch {0} : {1}  
PAM-CM-0247 = Message 32026: Patch with name {0} has been uploaded successfully.  
PAM-CM-0248 = Invalid file type of {0}. Import supports only CSV files of types: csv.  
PAM-CM-0249 = Need to provide /approve or /deny as path parameter.  
PAM-CM-0250 = Deleted Certificate: {0}  
PAM-CM-0251 = Error updating configuration (split tunnel)  
PAM-CM-0252 = Error updating configuration (net)  
PAM-CM-0253 = Mask must be integer number between 16 and 29 bits  
PAM-CM-0254 = Error updating configuration (mask)  
PAM-CM-0255 = SSL VPN Configuration updated; Network: {0}/{1}; Split tunneling enabled  
PAM-CM-0256 = SSL VPN Configuration updated; Network: {0}/{1}  
PAM-CM-0257 = Configuration updated  
PAM-CM-0258 = RSA authentication manager configuration file names must be sdconf.rec or sdopts.rec  
PAM-CM-0259 = BMC Remedy SDK file names must be arapi8\*.jar, arapi9\*.jar, arutil81\*.jar, or arutil91\*.jar.  
PAM-CM-0260 = Error uploading BMC Remedy SDK file {0}. Please check version.  
PAM-CM-0261 = CA Privileged Access Manager is collecting and analyzing limited information about your client system and sessions  
PAM-CM-0262 = Successfully connected to BAP server  
PAM-CM-0263 = Unable to retrieve Risk Levels from BAP server. Invalid or missing API token  
PAM-CM-0264 = Unable to retrieve Risk Levels from BAP server  
PAM-CM-0265 = Command String has been Enabled  
PAM-CM-0266 = Command String has been Disabled



PAM-CM-0267 = Invalid characters or extension in your filename! No spaces or special characters allowed.(Extension should be ".gz.bin" or ".cfg")

PAM-CM-0268 = File {0} uploaded successfully. You can use it to restore the Config now.

PAM-CM-0269 = File {0} uploaded successfully. You can use it to restore the Database now.

PAM-CM-0274 = FIPS mode can not be activated when logging to an external server is enabled. Disable external logging first

PAM-CM-0275 = Could not activate FIPS mode because SNMP is configured for unsecured access. Please configure SNMP (poll server and traps) for v3 access only and try again.

PAM-CM-0276 = Could not activate FIPS mode because CA PAM as a SAML SP is configured to accept assertions signed using a SHA1 based algorithm. SHA1 based algorithms are not supported in FIPS mode.

PAM-CM-0277 = Can not start Monitor. Please verify the information in General Monitoring Parameters.

PAM-CM-0278 = Can not stop Monitor

PAM-CM-0279 = The Email logs option may only be enabled if you have a valid Admin Email, SMTP Server, and Appliance From Address configured under the Monitor tab.

PAM-CM-0280 = "Date and Time","Private IP","Public IP","NAT/Proxy IP","User","Transaction","Address","Device Name","Port","Access/Protocol","Service/App","Details","Target Account","Password View Request ID"

PAM-CM-0281 = Attaching of additional storage attached to this virtual appliance ({0}) initiated, this appliance will be rebooted.

PAM-CM-0282 = Attachment of additional storage completed successfully

PAM-CM-0283 = Detaching of additional storage from this virtual appliance initiated, this appliance will be rebooted

PAM-CM-0284 = Downloaded database backup public key file {0}

PAM-CM-0285 = Error downloading database backup public key file: {0}

PAM-CM-0286 = Session recording purging settings updated.

PAM-CM-0287 = Problem changing the SNMP Agent startup flag: {0}

PAM-CM-0288 = SNMP Agent startup flag changed successfully. Start at boot: {0}

PAM-CM-0289 = Can not save SNMP daemon configuration: {0}

PAM-CM-0290 = SNMP poll configuration saved successfully. Read-only Community: {0}

PAM-CM-0291 = SNMP Agent started successfully

PAM-CM-0292 = Problem starting SNMP Agent: {0}

PAM-CM-0293 = SNMP Agent stopped successfully

PAM-CM-0294 = Problem stopping SNMP Agent: {0}

PAM-CM-0295 = Invalid characters for Read-Only Community

PAM-CM-0296 = xceedium is not a valid SNMPv3 username

PAM-CM-0297 = Invalid characters for SNMPv3 Username

PAM-CM-0298 = Authentication Passphrase must be at least eight (8) characters in length

PAM-CM-0299 = Private Passphrase can be omitted or should be at least eight (8) characters in length

PAM-CM-0300 = SNMPv3 User "{0}" already exists

PAM-CM-0301 = SNMPv3 user "{0}" added successfully

PAM-CM-0302 = SNMPv3 user "{0}" updated successfully

PAM-CM-0303 = SNMPv3 Username "{0}" not found

PAM-CM-0304 = SNMPv3 user "{0}" deleted successfully

PAM-CM-0305 = {0} has been loaded({1}){2}{3}

PAM-CM-0306 = Uploaded Certificate {0}

PAM-CM-0307 = Certificate ({0}) Self signed Certificate

PAM-CM-0309 = Uploaded Certificate with Private Key {0}

PAM-CM-0311 = {0} has been loaded

PAM-CM-0312 = Uploaded Intermediate Certificate {0}

PAM-CM-0313 = Could not activate FIPS mode because CA PAM as a SAML SP is configured to sign authentication requests to the the following SAML Remote IdPs using SHA1: {0}. SHA1 based algorithms are not supported in FIPS mode.

PAM-CM-0314 = Uploaded CA Bundles {0}

PAM-CM-0315 = Uploaded Certificate Revocation List {0}

PAM-CM-0316 = Please enter the same content in Passphrase and Confirm fields

PAM-CM-0317 = Certificate Upload: {0} ({1})  
PAM-CM-0318 = Certificate with Private Key Upload: This is not a PEM certificate ({0})  
PAM-CM-0319 = This is not a PEM certificate  
PAM-CM-0320 = Certificate with Private Key Upload: Error opening certificate. please check the certificate ({0})  
PAM-CM-0322 = Certificate with Private Key Upload: {0} ({1})  
PAM-CM-0323 = Certificate with Private Key Upload: PEM Private Key is missing ({0})  
PAM-CM-0324 = PEM Private Key is missing  
PAM-CM-0325 = Certificate with Private Key Upload: Private Key file encrypted, please provide Passphrase ({0})  
PAM-CM-0326 = Private Key file encrypted, please provide Passphrase  
PAM-CM-0327 = Certificate with Private Key Upload: Error occurred. Please check Passphrase ({0})  
PAM-CM-0328 = Error occurred. Please check Passphrase  
PAM-CM-0329 = Intermediate Certificate Upload: {0} ({1})  
PAM-CM-0330 = Intermediate Certificate Upload: Unknown format ({0})  
PAM-CM-0331 = Intermediate Certificate Upload: Invalid CA Certificate ({0})  
PAM-CM-0332 = Invalid CA Certificate  
PAM-CM-0333 = Intermediate Certificate Upload: Invalid Key Usage ({0})  
PAM-CM-0334 = Invalid Key Usage  
PAM-CM-0335 = CA Bundles Upload: {0} ({1})  
PAM-CM-0336 = CA Bundles Upload: Unknown Format ({0})  
PAM-CM-0337 = Certificate Revocation List Upload: Unknown Format ({0})  
PAM-CM-0338 = Certificate Revocation List Upload: Please choose downloaded CRL option and try again ({0})  
PAM-CM-0339 = Please choose downloaded CRL option and try again  
PAM-CM-0340 = Error: Certificate version {0} but contains x509v3 extensions. Ensure that x509v3 certificates show Version 3 in the Version field.  
PAM-CM-0341 = Certificate with Private Key Upload: Error: Certificate version {0} but contains x509v3 extensions. Ensure that x509v3 certificates show Version 3 in the Version field. ({1})  
PAM-CM-0342 = Error opening certificate. Please check the certificate  
PAM-CM-0343 = Certificate Upload: Error opening certificate. Please check the certificate ({0})  
PAM-CM-0344 = Certificate Upload: Error: Certificate version {0} but contains x509v3 extensions. Ensure that x509v3 certificates show Version 3 in the Version field. ({1})  
PAM-CM-0345 = Self signed Certificate  
PAM-CM-0346 = {0} has been verified  
PAM-CM-0347 = Rebooting after new certificate accepted  
PAM-CM-0348 = SAMPR log level not updated  
PAM-CM-0349 = {0} has been verified.  
PAM-CM-0350 = Object empty: Log  
PAM-CM-0351 = Date/Time changed successfully. New time: {0, date, MM-dd-yyyy HH:mm} in Timezone: {1}.  
PAM-CM-0352 = Unable to change Date/Time: {0}  
PAM-CM-0353 = Time Servers information updated successfully  
PAM-CM-0354 = Updated Time Servers. Synchronize at boot: Enabled, Servers: {0}.  
PAM-CM-0355 = Updated Time Servers. Synchronize at boot: Disabled, Servers: {0}.  
PAM-CM-0356 = Error updating Time Servers information: {0}  
PAM-CM-0357 = NTP IFF key saved: closed security policy no key  
PAM-CM-0358 = NTP IFF key saved: closed security policy  
PAM-CM-0359 = NTP IFF key saved: open security policy no key  
PAM-CM-0360 = NTP IFF key saved: open security policy

## **SSH Certificate Policy Messages**

- PAM-CM-1892=The SSH Certificate Policy ID is missing.
- PAM-CM-1893=The specified SSH Certificate Policy ID is invalid; it must be an integer greater than zero.
- PAM-CM-1894=The SSH Certificate Policy name is missing.
- PAM-CM-1895=The specified SSH Certificate Policy name is invalid; it must consist of characters [a-z, A-Z, 0-9].
- PAM-CM-1896=The specified SSH Certificate Policy name is too long; reduce the number of characters that it contains.
- PAM-CM-1897=The SSH Certificate Policy description is missing.
- PAM-CM-1898=The SSH Certificate Policy description is invalid; it must consist of characters [a-z, A-Z, 0-9].
- PAM-CM-1899=The SSH Certificate Policy description is too long; reduce the number of characters that it contains.
- PAM-CM-1900=The SSH Certificate Policy force command is too long; reduce the number of characters that it contains.
- PAM-CM-1901=The specified SSH Certificate Policy permit-x11-forwarding is invalid; it must be true or false.
- PAM-CM-1902=The specified SSH Certificate Policy permit-pty is invalid; it must be true or false.
- PAM-CM-1903=The specified SSH Certificate Policy permit-port-forwarding is invalid; it must be true or false.
- PAM-CM-1904=The specified SSH Certificate Policy permit-user-rc is invalid; it must be true or false.
- PAM-CM-1905= An SSH Certificate Policy ID or Name must be specified.
- PAM-CM-1906=Failed to load an SSH Certificate Policy having the specified ID or Name.
- PAM-CM-1907=Must specify either an SSH Certificate Policy ID or a Name but not both.
- PAM-CM-1908=Failed to add an SSH Certificate Policy having the specified ID or Name.
- PAM-CM-1909=The SSH Certificate Policy permit-x11-forwarding is missing.
- PAM-CM-1910=The SSH Certificate Policy permit-pty is missing.
- PAM-CM-1911=The SSH Certificate Policy permit-port-forwarding is missing.
- PAM-CM-1912=The SSH Certificate Policy permit-user-rc is missing.
- PAM-CM-1913=Cannot delete Default policy.
- PAM-CM-1914=Cannot update Default policy's name.

## **PAM-CMN: Common Messages**

Messages display a category in the second group of letters in the message. For example, PAM-CMN refers to Common errors. Common Messages is the largest category, so it is divided into smaller categories which are described individually in the topics in this section.

**Use the table of contents to access the common message category topics.**

### **Other Message Categories**

- CLNT = CA PAM Client
- CM = Credential Manager
- LDAP = LDAP Importer
- MGC = Management Console
- PRX = Proxy
- SPFD = Secure Port Forwarding Daemon
- SRM = Session Recording Manager
- UI = User Interface
- UPD = Session Clean-up and Storage Status Messages

## General Error Messages

PAM-CMN-0000 = Error occurred while trying to complete request. ({0})  
PAM-CMN-0001 = Expected an array {0}, got a scalar.  
PAM-CMN-0002 = Values {0} must be either 't' (true) or 'f' (false).  
PAM-CMN-0003 = Not authorized to perform this action.  
PAM-CMN-0004 = Unable to retrieve Privilege Manager.  
PAM-CMN-0005 = Privilege Manager unable to retrieve user.  
PAM-CMN-0006 = Cannot build Privilege Manager with data supplied.  
PAM-CMN-0007 = Invalid numeric data. {0}  
PAM-CMN-0008 = Invalid sort order  
PAM-CMN-0009 = Your login has timed out.  
PAM-CMN-0010 = Error occurred while trying to complete request.  
PAM-CMN-0011 = Invalid log database type {0}. Consult your system administrator  
PAM-CMN-0012 = Invalid search by field {0}  
PAM-CMN-0013 = No more rows.  
PAM-CMN-0014 = Same origin policy violation; possible cross-site request forgery.  
PAM-CMN-0015 = Too many rows to sort by. Use search criteria to narrow the result set and try again.  
PAM-CMN-0016 = All Devices  
PAM-CMN-0017 = All Users  
PAM-CMN-0018 = Duplicate entry  
PAM-CMN-0019 = Missing required field {0}  
PAM-CMN-0020 = Error occurred while trying to complete request. ({0})  
PAM-CMN-0021 = No data returned.  
PAM-CMN-0022 = SSH login to appliance from address {0}.

## Message Fragments Used by Other Messages

PAM-CMN-0023 = add  
PAM-CMN-0024 = update  
PAM-CMN-0025 = delete  
PAM-CMN-0026 = user groups  
PAM-CMN-0027 = device groups  
PAM-CMN-0028 = Connected  
PAM-CMN-0029 = Waiting  
PAM-CMN-0030 = Unknown  
PAM-CMN-0031 = Detection  
PAM-CMN-0032 = Intervention  
PAM-CMN-0033 = Tampering  
PAM-CMN-0034 = Password Authority Groups  
PAM-CMN-0035 = VMware provisioning request  
PAM-CMN-0036 = Activated  
PAM-CMN-0037 = Deactivated

## Network Service Messages

PAM-CMN-0038 = Service name is required.  
PAM-CMN-0039 = Local IP address is required.  
PAM-CMN-0040 = Invalid IP address specified.  
PAM-CMN-0041 = Protocol is required.  
PAM-CMN-0042 = Invalid protocol specified.  
PAM-CMN-0043 = Web Portal is required.  
PAM-CMN-0044 = Invalid Web Portal value specified.

PAM-CMN-0045 = Show in Column is required.  
PAM-CMN-0046 = Invalid Show in Column value specified.  
PAM-CMN-0047 = Enabled is required.  
PAM-CMN-0048 = Invalid Enabled value specified.  
PAM-CMN-0049 = Port settings are required.  
PAM-CMN-0050 = Invalid port setting(s) specified: {0}.  
PAM-CMN-0051 = Application protocol is required.  
PAM-CMN-0052 = Invalid application protocol value specified.  
PAM-CMN-0053 = Launch URL is required.  
PAM-CMN-0054 = Invalid launch URL specified.  
PAM-CMN-0055 = Invalid characters in comment.  
PAM-CMN-0056 = Invalid characters in service name. Semicolons, commas, percent signs, and backslashes are invalid.  
PAM-CMN-0057 = Existing service could not be found.  
PAM-CMN-0058 = Service {0} already exists.  
PAM-CMN-0059 = Service {0} created.  
PAM-CMN-0060 = Unable to delete service. Service does not exist.  
PAM-CMN-0061 = Service deleted.  
PAM-CMN-0062 = Service name cannot be changed.  
PAM-CMN-0063 = SSL VPN service must have at least 1 port defined.  
PAM-CMN-0064 = Invalid TCP ports value specified. Values must be valid TCP ports or TCP port ranges.  
PAM-CMN-0065 = Invalid UDP ports value specified. Values must be valid UDP ports or UDP port ranges.  
PAM-CMN-0066 = Service not found.  
PAM-CMN-0067 = Service {0} updated.  
PAM-CMN-0068 = Unrecognized service type.  
PAM-CMN-0069 = Invalid port range specified. {0} greater than {1}.  
PAM-CMN-0070 = Maximum number of ports in range, 500, exceeded for specified port range {0}. Consider using SSL VPN solution.  
PAM-CMN-0071 = Invalid port combination/redirection {0}. Combination/redirection format should be <Remote Port>:<Local Port>.  
PAM-CMN-0072 = Local IP must be on the 127 network.  
PAM-CMN-0073 = Web portal TCP/UDP services must have LeapFrog Prevention disabled.  
PAM-CMN-0074 = Web portal TCP/UDP services cannot have a client application.  
PAM-CMN-0075 = Launch path is required.  
PAM-CMN-0076 = Service not added.  
PAM-CMN-0077 = Database corruption - more than one service was inserted.  
PAM-CMN-0078 = Service {0} not found or another user deleted it.  
PAM-CMN-0079 = Database corruption - more than one service with the same id was deleted.  
PAM-CMN-0080 = {0} service(s) deleted  
PAM-CMN-0081 = {0} service(s) not deleted because not authorized.  
PAM-CMN-0082 = {0} service(s) not deleted because not found.  
PAM-CMN-0083 = {0} service(s) not deleted because of unknown error.  
PAM-CMN-0084 = {0} service(s) deleted {1} {2} {3}  
PAM-CMN-0085 = Only the Local IP, Port Settings, Enabled, Show in Column, Client Application, and Comments of the standard service sftpftp can be updated.  
PAM-CMN-0086 = Only the Local IP, Port Settings, Enabled, Show in Column, and Comments of the standard service sftpftpemb can be updated.  
PAM-CMN-0087 = Only the Local IP, Port Settings, Enabled, Show in Column, and Comments of the standard service TSWEB can be updated.  
PAM-CMN-0088 = Standard service sftpftp can not be deleted.  
PAM-CMN-0089 = Standard service sftpftpemb can not be deleted.  
PAM-CMN-0090 = Standard service TSWEB can not be deleted.  
PAM-CMN-0091 = Standard service sftpsftp can not be deleted.



PAM-CMN-0092 = Only the Local IP, Port Settings, Enabled, Show in Column, Client Application, and Comments of the standard service sftpsftp can be updated.

PAM-CMN-0093 = Local socket {0}:{1} of Web Portal {2} must be unique across all web portal services. Local socket already used by Web Portal {3}.

PAM-CMN-0094 = Standard service sftpsftpemb can not be deleted.

PAM-CMN-0095 = Only the Local IP, Port Settings, Enabled, Show in Column, and Comments of the standard service sftpsftpemb can be updated.

PAM-CMN-0096 = Invalid Hide Web Portal specified.

PAM-CMN-0097 = Hide Web Portal is required.

PAM-CMN-0098 = Both Show In Column and Hide Web Portal cannot be checked.

PAM-CMN-0099 = Maximum number of ports in range, 500, exceeded for the sum of all specified port ranges. Consider using SSL VPN solution.

PAM-CMN-0100 = A web application must have an application protocol of 'Web Portal'.

PAM-CMN-0101 = Invalid web portal browser type specified. Valid types are native and CA.

PAM-CMN-0102 = Invalid domain in web portal access list: {0}.

PAM-CMN-0103 = AWS Management Console SSO service can not be deleted.

PAM-CMN-0104 = AWS Management Console SSO is a reserved service name.

PAM-CMN-0105 = The only properties of the AWS Management Console SSO service that can be changed are enabled, show in column, and access list.

PAM-CMN-0106 = MS Office 365 is a reserved service name.

PAM-CMN-0107 = MS Office 365 service can not be deleted.

PAM-CMN-0108 = AWS Proxy Service is a reserved service name.

PAM-CMN-0109 = The properties of the AWS proxy service can not be changed.

PAM-CMN-0110 = The only properties of the MS Office 365 service that can be changed are enabled, show in column, and access list.

PAM-CMN-0111 = AWS Proxy service can not be deleted.

PAM-CMN-0112 = At least one SAML Subject Name Identifier Format must be selected for the SAML service.

PAM-CMN-0113 = SAML Entity ID is a required field.

PAM-CMN-0114 = SAML PEM Certificate is a required field.

PAM-CMN-0115 = The specified SAML {0} certificate is not a valid PEM encoded certificate.

PAM-CMN-0116 = The SAML encryption type is a required field.

PAM-CMN-0117 = The SAML initiating party field is invalid: Valid values are sp or idp.

PAM-CMN-0118 = Invalid SAML encryption type. Valid values are: None,Nameld,Assertion.

PAM-CMN-0119 = A SAML service with an entity ID of {0} already exists. SAML entity IDs must be unique.

PAM-CMN-0120 = An error occurred while parsing the SAML metadata file: {0}

PAM-CMN-0121 = {0} service cannot not be deleted.

PAM-CMN-0122 = Invalid SAML require signed authentication request value specified. Valid values are: t, f.

PAM-CMN-0123 = The SAML encryption certificate is required if Nameld or Assertion encryption is enabled.

PAM-CMN-0124 = The SAML signing certificate is required if Require Signed Authn Requests is enabled.

PAM-CMN-0125 = There are no SAML 2.0 SPs defined with binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST (SAML 1.1 SPs are not supported).

PAM-CMN-0126 = CA PAM requires an AssertionConsumerService element with binding urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.

PAM-CMN-0127 = SAML service {0} with entity ID {1} {2}.

PAM-CMN-0128 = The following device(s) were {0} to host the SAML assertion consumer services: {1}.

PAM-CMN-0129 = Device group {0} was provisioned with the provisioned assertion consumer devices as members. This will facilitate managing policy for all SAML devices.

PAM-CMN-0130 = SAML attribute with index {0} is missing the required name field.

PAM-CMN-0131 = SAML attribute with index {0} is missing the required friendly name field.

PAM-CMN-0132 = There are multiple SAML attributes with the same name: {0}. Names must be unique.

PAM-CMN-0133 = There are multiple SAML attributes with the same friendly name: {0}. Friendly names must be unique.

PAM-CMN-0134 = SAML attribute {0} can not be deleted. It is used in the following policies: {1}.

PAM-CMN-0135 = The following SAML Name Identifier Formats can not be deleted: {0}. They are used in the following policies: {1}.

PAM-CMN-0136 = The auto-login method of SAML services can not be changed.

PAM-CMN-0137 = Invalid web portal auto-login method specified.

PAM-CMN-0138 = SAML services with the Route Through CA PAM setting enabled require the browser type setting to be set to the CA Browser.

PAM-CMN-0139 = SAML services using the CA browser must be IdP initiated.

PAM-CMN-0140 = VMware NSX API Proxy Service is a reserved service name.

PAM-CMN-0141 = An auto-login method was provided, but only web portals can have auto-login methods.

PAM-CMN-0142 = This service is configured to be recorded and must use the CA browser type. The service is configured to be recorded in the following policies: {0}.

PAM-CMN-0143 = SAML service data is not valid

## User Management Messages

PAM-CMN-0144 = User id must be a positive integer.

PAM-CMN-0145 = User {0} not found.

PAM-CMN-0146 = The super user may not be deleted.

PAM-CMN-0147 = User {0} deleted.

PAM-CMN-0148 = User {0} not found or another user deleted them.

PAM-CMN-0149 = Database corruption - more than one user with the same id was deleted.

PAM-CMN-0150 = User or user group {0} already exists. Names must be unique.

PAM-CMN-0151 = User {0} added.

PAM-CMN-0152 = User {0} not added.

PAM-CMN-0153 = Database corruption - more than one user was inserted.

PAM-CMN-0154 = User {0} updated.

PAM-CMN-0155 = User {0} was not updated.

PAM-CMN-0156 = Database corruption - more than one user was updated.

PAM-CMN-0157 = Access time day string is 7 digits long; 1 = access permitted 0 = access forbidden.

PAM-CMN-0158 = AD Indirect Flag must be 0 or 1.

PAM-CMN-0159 = {0} time invalid.

PAM-CMN-0160 = From time must be earlier than To time.

PAM-CMN-0161 = Invalid characters in user name {0}. Semicolons, commas, percent signs, single and double quotes, and backslashes are invalid.

PAM-CMN-0162 = First name is a required field.

PAM-CMN-0163 = Last name is a required field.

PAM-CMN-0164 = Email is a required field.

PAM-CMN-0165 = Invalid email address.

PAM-CMN-0166 = Password is a required field.

PAM-CMN-0167 = Special characters quote, double quote, backslash, and percent are not allowed in the password.

PAM-CMN-0168 = Password length must be between {0} and {1} characters long.

PAM-CMN-0169 = Password must include both an alphabetic and a numeric character.

PAM-CMN-0170 = Password must include both upper and lower case alphabetic characters.

PAM-CMN-0171 = Password must include a special character ~!?'@#\$%^&\*()\_+=+;,,<>{}|/-.[].

PAM-CMN-0172 = Password must include at least two lowercase letters, two uppercase letters, two numbers and two special characters.

PAM-CMN-0173 = Authorization must be Local, RSA, PKI, RADIUS, or LDAP.

PAM-CMN-0174 = Password reset flag must be set on when creating a user.

PAM-CMN-0175 = Active flag must be true or false.

PAM-CMN-0176 = Database corruption - active flag not >= -1.

PAM-CMN-0177 = Expiration date must be in the future or not set.

PAM-CMN-0178 = Role structure passed in is incorrect - missing {0}.

PAM-CMN-0179 = User must belong to one of the following groups {0}.

PAM-CMN-0180 = Your role does not allow you to {0} this user without any groups.

PAM-CMN-0181 = You may only add users to the following groups {0}.

PAM-CMN-0182 = You may not delete this user. You may only remove group assignments from it.

PAM-CMN-0183 = {0} user(s) deleted.

PAM-CMN-0184 = {0} user(s) deleted, {1} user(s) not deleted.

PAM-CMN-0185 = User or group name may not be changed from {0}.

PAM-CMN-0186 = Virtual user flag must be 1 (true), or 0 (false).

PAM-CMN-0187 = Invalid access time passed in. Missing a required key field.

PAM-CMN-0188 = Malformed user group structure. See log for details.

PAM-CMN-0189 = Invalid provisioning type {0}.

PAM-CMN-0190 = User super may not have its roles changed.

PAM-CMN-0191 = Non-local users may not have passwords defined in CA PAM.

PAM-CMN-0192 = {0} users attempted, {1} users successfully added, {2} users not added.

PAM-CMN-0193 = Short name may only be used for users with provision type of LDAP or PKI.

PAM-CMN-0194 = Short name required for an LDAP provisioned user.

PAM-CMN-0195 = Provision type may not be changed.

PAM-CMN-0196 = Invalid user type.

PAM-CMN-0197 = Active flag is required.

PAM-CMN-0198 = PAP/CHAP must be specified for RADIUS authentication and only for RADIUS authentication.

PAM-CMN-0199 = Warning: Global administrators may not have limited access times - any such settings will be ignored.

PAM-CMN-0200 = {0} user(s) were requested to be enabled, {1} user(s) were actually enabled.

PAM-CMN-0201 = An invisible (shadow) user named {0} already exists. Please choose another name.

PAM-CMN-0202 = A user or group named {0} already exists. Please contact your system administrator.

PAM-CMN-0203 = {0} user(s) not deleted because not authorized.

PAM-CMN-0204 = {0} user(s) not deleted because not found.

PAM-CMN-0205 = {0} user(s) not deleted because of unknown error.

PAM-CMN-0206 = {0} user(s) deleted {1} {2} {3} {4} {5}

PAM-CMN-0207 = Can't specify the user as their own login contact. Use the Email Self on Login checkbox.

PAM-CMN-0208 = Login contact {0} not found.

PAM-CMN-0209 = Users provisioned from LDAP may not be deleted directly, only by deleting their LDAP group.

PAM-CMN-0210 = {0} LDAP users not deleted

PAM-CMN-0211 = User names, group names, and short names may not be the same.

PAM-CMN-0212 = Inconsistent provision and authentication types.

PAM-CMN-0213 = Inconsistent data - a source user cannot be provided on an update.

PAM-CMN-0214 = Invalid User Id provided for copy

PAM-CMN-0215 = Unauthorized attempt to retrieve the list of users.

PAM-CMN-0216 = Unauthorized attempt to add a user.

PAM-CMN-0217 = Unauthorized attempt to assign a user to a group.

PAM-CMN-0218 = Unauthorized attempt to retrieve user details.

PAM-CMN-0219 = Unauthorized attempt to delete user from group(s).

PAM-CMN-0220 = Unauthorized attempt to delete user.

PAM-CMN-0221 = Unauthorized attempt to update global administrator account.

PAM-CMN-0222 = Unauthorized attempt to update a user.

PAM-CMN-0223 = Unauthorized attempt to update user's properties.

PAM-CMN-0224 = Unauthorized attempt to reactivate user(s).

PAM-CMN-0225 = Invalid RDP user name {0}.

PAM-CMN-0226 = Mainframe Display Name entry has invalid characters. Allowed characters are (alpha, numeric, underscore)

PAM-CMN-0227 = Unauthorized attempt to view the effective policy of user {0}.

PAM-CMN-0228 = An LDAP provisioned user may not be added directly, only imported via LDAP.

PAM-CMN-0229 = LDAP-provisioned user {0}'s LDAP groups may not be changed except via LDAP import or refresh.

PAM-CMN-0230 = Shadow user {0}'s membership in RADIUS group {1} may not be changed.



PAM-CMN-0231 = A shadow user may not be added directly, only created via logon.

PAM-CMN-0232 = User {0} may not be added to RADIUS group {1}.

PAM-CMN-0233 = Duplicate Password Authority username {0}. User not added. Please contact your system administrator.

PAM-CMN-0234 = User add failed. Please contact your system administrator.

PAM-CMN-0235 = User is not allowed to manage the Password Authority group {0}.

PAM-CMN-0236 = Roles with the Manage Credential privilege must have at least one Password Authority group to manage.

PAM-CMN-0237 = Password Authority user group name {0} not found.

PAM-CMN-0238 = Super user cannot change Password Authority user groups.

PAM-CMN-0239 = User {0} cannot be deleted because of a Password Authority error.

PAM-CMN-0240 = Duplicate user principal name {0}. User cannot be {1}.

PAM-CMN-0241 = Devices provisioned from LDAP may not be deleted directly, only by deleting their LDAP group.

PAM-CMN-0242 = The user has been configured to manage a Password Authority group but does not have a role with sufficient privileges.

PAM-CMN-0243 = Maximum of {0} AWS API Proxy users licensed. Please remove that privilege from one or more users before proceeding to add this one.

PAM-CMN-0244 = API keys must be an array of arrays of individual API keys containing id, name, target account id, active status and set of roles.

PAM-CMN-0245 = Required API key array element client name not found.

PAM-CMN-0246 = Required API key array element target account id not found.

PAM-CMN-0247 = Required API key array element isActive not found.

PAM-CMN-0248 = Required API key array element roles not found.

PAM-CMN-0249 = API key array element roles must be an array.

PAM-CMN-0250 = API keys must be deleted before the rest of the user.

PAM-CMN-0251 = Existing API key {0} either does not belong to user {1} or does not exist at all.

PAM-CMN-0252 = Users with provision type {0} can not be added to LDAP groups: {1}.

PAM-CMN-0253 = The following user ids are not valid: {0}.

PAM-CMN-0254 = You cannot specify an API key id when creating a user.

PAM-CMN-0255 = Pap/Chap must be null if authentication type is not radius or tacacs.

PAM-CMN-0256 = A user may not be locally added to an LDAP provisioned group.

PAM-CMN-0257 = The following user fields may not be changed locally for an ldap user: activationDate, authType, description, email, expiration, firstName, lastName, password, phone, resetPasswordFlag.

PAM-CMN-0258 = A valid password is required. Empty passwords not allowed.

PAM-CMN-0259 = User not found.

PAM-CMN-0260 = Maximum length of email field is 60 characters.

PAM-CMN-0261 = The super user account's authentication method cannot be set to SAML.

PAM-CMN-0262 = A user may not have two API keys with the same name. Change the API keys so that only one is named {0}.

PAM-CMN-0263 = User with local authentication must have a password set.

PAM-CMN-0264 = Password has been already used. You have to enter a new password.

PAM-CMN-0265 = Invalid old password.

PAM-CMN-0266 = Password must be new

PAM-CMN-0267 = Special characters " ' % and are not allowed in the password

PAM-CMN-0268 = Password length must be "{0}" - "{1}" characters.

PAM-CMN-0269 = Must include both an alphabetic and numeric character.

PAM-CMN-0270 = Must include both upper and lower case alphabetic characters.

PAM-CMN-0271 = Must include a special character ~!?'@#\$%^&\*()\_+=+;,<.>{}|/[-[]

PAM-CMN-0272 = Password must include at least two lowercase letters, two uppercase letters, two numbers and two special characters.

PAM-CMN-0273 = User {0} must be associated with Password Authority user group {1}.

PAM-CMN-0274 = The old password you entered is not correct.

PAM-CMN-0275 = Password change failed. Unknown error.

PAM-CMN-0276 = User groups for a SAML JIT user can only be changed by SAML.

PAM-CMN-0277 = A {0} provisioned user must belong to at least one group.

PAM-CMN-0278 = A SAML JIT user such as {0} can only have their user groups changed by SAML.

PAM-CMN-0279 = A SAML JIT user like {0} may not be added directly, only loaded from an identity provider on login.

PAM-CMN-0280 = User {0} cannot be deleted because it is configured as the login contact for the following list of users: {1}.

PAM-CMN-0281 = {0} user(s) configured as login contact(s) not deleted

PAM-CMN-0282 = The user has been assigned a role which requires a password authority user group to be associated with it, but no such group was specified.

PAM-CMN-5405 = Unable to delete user, because it is configured for Forced Deactivation Alert.

PAM-CMN-5470="User deactivation reason set to others."

PAM-CMN-5471="User deactivation reason is cleared."

PAM-CMN-5472="User deactivation reason must be 0 (Others) or 1 (Inactivity)."

PAM-CMN-5473="Failed to update login history for user {1}."

PAM-CMN-5600="Invalid value specified for Disable Inactive After. The value for Disable Inactive After must be greater than the value for Remind Before Deactivation."

PAM-CMN-5601="Invalid value specified for Remind Before Deactivation. The value must be greater than zero."

PAM-CM-6001: {0} inactive user(s) have been auto deactivated for exceeding maximum allowable inactivity period of {1} day(s).

PAM-CM-6002: Deactivation reminder notification email has been sent to {0} inactive user(s).

PAM-CM-6003: Inactive users are deactivated on-demand.

PAM-CM-6004: Deactivation reminder notification emails have been sent on-demand.

PAM-CM-6005: Failed to deactivate inactive users on-demand.

PAM-CM-6006: Failed to send deactivation reminder notification emails on-demand.

PAM-CM-6007: Deactivation notification email has been sent to {0} deactivated user(s).

PAM-CM-6008: Failed to send deactivation notification email. Please check the email server configuration.

PAM-CM-6009: Failed to send deactivation reminder notification email. Please check the email server configuration.

PAM-CM-6010: Started the user deactivation reminder task.

PAM-CM-6011: No users were found that require a deactivation reminder.

PAM-CM-6012: Started the user deactivation task.

PAM-CM-6013: No users were found that require deactivation.

PAM-CM-6014: Failed to run the user deactivation task.

## Smart Button Group Messages

PAM-CMN-0283 = Smart button group name is required.

PAM-CMN-0284 = Invalid smart button group configuration file id specified.

PAM-CMN-0285 = Smart button group id required.

PAM-CMN-0286 = Invalid smart button group users specified.

PAM-CMN-0287 = Invalid smart button group id specified.

PAM-CMN-0288 = Invalid smart button group description specified.

PAM-CMN-0289 = A smart button group with name {0} already exists.

PAM-CMN-0290 = Invalid smart button group configuration file id specified.

PAM-CMN-0291 = Smart button group {0} not found.

PAM-CMN-1358 = Unexpected result from deleting smart button group

PAM-CMN-1456 = Successfully deleted selected Smart Button group {0}.

PAM-CMN-1551 = Unauthorized attempt to update smart button group {0} by {1}

PAM-CMN-1552 = Unauthorized attempt to add smart button group {0} by user {1}

PAM-CMN-1553 = Smart Button group {0} added.

PAM-CMN-1554 = Smart Button group {0} not added

PAM-CMN-1555 = Database corruption - more than one Smart Button group was added  
PAM-CMN-1556 = Unauthorized attempt to delete smart button group {0} by {1}  
PAM-CMN-1557 = Successfully deleted smart button group {0}  
PAM-CMN-1558 = Smart Button group {0} was not found and not deleted  
PAM-CMN-1559 = Unexpected result from deleting smart button group  
  
PAM-CMN-1590 = User {0} tried to retrieve the list of smart button groups without authorization  
  
PAM-CMN-2400 = Smart Button group {0} updated  
PAM-CMN-2401 = Database corruption - more than one Smart Button group was updated  
PAM-CMN-2402 = Smart Button group {0} updated, but users: {1} already belong to a smart button group

## User Group Management Messages

PAM-CMN-0292 = User group id must be a positive integer.  
PAM-CMN-0293 = User group not found.  
PAM-CMN-0294 = User group {0} deleted.  
PAM-CMN-0295 = User group {0} not found or another user deleted it.  
PAM-CMN-0296 = Database corruption - more than one user group with the same id was deleted.  
PAM-CMN-0297 = User group or user {0} already exists. Names must be unique.  
PAM-CMN-0298 = User group {0} added.  
PAM-CMN-0299 = User group {0} not inserted.  
PAM-CMN-0300 = Database corruption - more than one user group with the same id was inserted.  
PAM-CMN-0301 = User group {0} updated.  
PAM-CMN-0302 = User group {0} was not updated.  
PAM-CMN-0303 = Database corruption - more than one user group with the same id was updated.  
PAM-CMN-0304 = Invalid user group type.  
PAM-CMN-0305 = User group name may not be blank.  
PAM-CMN-0306 = {0} user group(s) deleted.  
PAM-CMN-0307 = {0} user group(s) deleted, {1} user group(s) not deleted.  
PAM-CMN-0308 = User group not deleted.  
PAM-CMN-0309 = {0} user group(s) not deleted because not authorized.  
PAM-CMN-0310 = {0} user group(s) not deleted because not found.  
PAM-CMN-0311 = {0} user group(s) not deleted because of unknown error.  
PAM-CMN-0312 = {0} user group(s) deleted. {1} {2} {3}  
PAM-CMN-0313 = Unspecified user group name.  
PAM-CMN-0314 = Locally provisioned user groups can not have an authentication type of RSA.  
PAM-CMN-0315 = Locally provisioned user groups can not have an authentication type of LDAP+RSA.  
PAM-CMN-0316 = Invalid network range. {0}  
PAM-CMN-0317 = Locally provisioned user groups can not have an authentication type of LDAP+RADIUS.  
PAM-CMN-0318 = The following user group ids are not valid: {0}.  
PAM-CMN-0319 = Auth type {0} not supported.  
PAM-CMN-0320 = User {0} not successfully added to user group. No other users added.  
PAM-CMN-0321 = The following user fields may not be changed locally for an LDAP user group: description, shortName.  
PAM-CMN-0322 = Group id is required for an update and must be an integer > 0.

## Device Management Messages

PAM-CMN-0323 = Power must be On, Off, or Unknown.  
PAM-CMN-0324 = Device {0} not found.  
PAM-CMN-0325 = Device task enabled must be On or Off.  
PAM-CMN-0326 = Device property terminal customization must be 0 or 1.

PAM-CMN-0327 = Device property endselect must be 0 or 1.  
PAM-CMN-0328 = Device console type must be KDM, PPP, or Serial.  
PAM-CMN-0329 = Device service enabled must be On or Off.  
PAM-CMN-0330 = Device {0} deleted.  
PAM-CMN-0331 = Device {0} not found or another user deleted them.  
PAM-CMN-0332 = Database corruption - more than one device with the same id was deleted.  
PAM-CMN-0333 = Device or device group name {0} already exists. Names must be unique.  
PAM-CMN-0334 = Device {0} added.  
PAM-CMN-0335 = Device {0} not added.  
PAM-CMN-0336 = Database corruption - more than one device with the same id was inserted.  
PAM-CMN-0337 = Device {0} updated.  
PAM-CMN-0338 = Device {0} was not updated due to Password Authority authorization errors.  
PAM-CMN-0339 = Database corruption - more than one device with the same id was updated.  
PAM-CMN-0340 = Device {0} power status updated.  
PAM-CMN-0341 = Device {0} power status was not updated.  
PAM-CMN-0342 = Database corruption - more than one device's power status was updated.  
PAM-CMN-0343 = {0} {1} {2} Failed.  
PAM-CMN-0344 = {0} {1} {2} Successful.  
PAM-CMN-0345 = Unknown power status of {0}: multiple power ports do not match.  
PAM-CMN-0346 = Unsuccessful checking power status of {0}.  
PAM-CMN-0347 = Special type device {0} already exists.  
PAM-CMN-0348 = Special type device not found.  
PAM-CMN-0349 = Special type device {0} not inserted.  
PAM-CMN-0350 = Database corruption - more than one special type device was inserted.  
PAM-CMN-0351 = Special type device {0} was not updated.  
PAM-CMN-0352 = Database corruption - more than one special type device was updated.  
PAM-CMN-0353 = Device group name is required.  
PAM-CMN-0354 = Device domain name is required.  
PAM-CMN-0355 = A device must belong to one of the following groups {0}.  
PAM-CMN-0356 = Your role does not allow you to {0} this device without any groups.  
PAM-CMN-0357 = You may only add or delete device membership from the following groups {0}.  
PAM-CMN-0358 = You may not delete this device, only remove group assignments from it.  
PAM-CMN-0359 = Device name may not be blank.  
PAM-CMN-0360 = {0} device(s) deleted.  
PAM-CMN-0361 = {0} device(s) deleted, {1} device(s) not deleted.  
PAM-CMN-0362 = Device special type must be specified.  
PAM-CMN-0363 = Invalid device special type specified.  
PAM-CMN-0364 = Operating System is a required field.  
PAM-CMN-0365 = Invalid operating system specified.  
PAM-CMN-0366 = Invalid device id(s) {0}.  
PAM-CMN-0367 = Device terminal data is required.  
PAM-CMN-0368 = Device terminal type is required.  
PAM-CMN-0369 = Device terminal type is invalid: {0}.  
PAM-CMN-0370 = Device terminal type was not added.  
PAM-CMN-0371 = Configuring device {0} as a {1} device will exceed the number of licensed {2} devices.  
PAM-CMN-0372 = Expect string must be specified for all expect/response pairs.  
PAM-CMN-0373 = User requires Device/Group Manager or Delegated Administrator role to add discovered devices to CA PAM.  
PAM-CMN-0374 = Device cannot have both sftpftp and sftpftplib services.  
PAM-CMN-0375 = {0} device(s) not deleted because not authorized.  
PAM-CMN-0376 = {0} device(s) not deleted because not found.  
PAM-CMN-0377 = {0} device(s) not deleted because of unknown error.  
PAM-CMN-0378 = {0} device(s) deleted {1} {2} {3}

PAM-CMN-0379 = Invalid characters in device name {0}. Semicolons, commas, apostrophes and backslashes are invalid.

PAM-CMN-0380 = Task {0} port setting, {1}, already in use on device.

PAM-CMN-0381 = Mainframe access methods are not permitted without a Mainframe-capable license.

PAM-CMN-0382 = Access method {0} has duplicate name {1}.

PAM-CMN-0383 = Multiple access methods of type {0} must have different names.

PAM-CMN-0384 = Device cannot have both sftpsftp and sftpsftpemb services.

PAM-CMN-0385 = A custom name for a device task may not have colons, semicolons, commas, or backslashes.

PAM-CMN-0386 = Device cannot have both telnet and ssh2telnet access methods.

PAM-CMN-0387 = Invalid tag format

PAM-CMN-0388 = Tag {0} can not be deleted

PAM-CMN-0389 = {0} Tags deleted out of {1} requested

PAM-CMN-0390 = Tag {0} was NOT renamed to {1}

PAM-CMN-0391 = Maximum number of ports in range, 500, exceeded for specified port range {0}.

PAM-CMN-0392 = Port {0} out of range. Must be less than {1}.

PAM-CMN-0393 = Port {0} out of range. Must be greater than {1}.

PAM-CMN-0394 = No access is currently permitted because this CA PAM appliance is over-provisioned. Please contact your systems administrator.

PAM-CMN-0395 = This CA Privileged Access Manager appliance currently has more Devices defined than the configured license permits. Please either obtain a new license from Broadcom support or delete devices to bring this appliance back within its license constraints. Access is disabled until this is remediated.

PAM-CMN-0396 = Each power task must have a unique combination of power device and port.

PAM-CMN-0397 = Maximum number of ports in range, 500, exceeded for all specified port ranges.

PAM-CMN-0398 = Invalid value for device type Access.

PAM-CMN-0399 = Invalid value for device type Password Management.

PAM-CMN-0400 = Invalid value for device type A2A.

PAM-CMN-0401 = Request server type must be CLIENT or AGENT.

PAM-CMN-0402 = Invalid value for host name preserved.

PAM-CMN-0403 = Invalid value for autopatch.

PAM-CMN-0404 = Invalid value for request server active flag.

PAM-CMN-0405 = Invalid value for device type search.

PAM-CMN-0406 = Invalid value for request server id.

PAM-CMN-0407 = Request server id required for autoregistration.

PAM-CMN-0408 = Can't assign request server id to a device that is not a request server.

PAM-CMN-0409 = Operation aborted because Password Authority request server cannot be deleted. See log for details.

PAM-CMN-0410 = Operation aborted because Password Authority target server cannot be deleted. See log for details.

PAM-CMN-0411 = Device {0} not deleted because of Password Authority errors.

PAM-CMN-0412 = Device Import cannot add virtual devices only update them. Device Name = {0}.

PAM-CMN-0413 = Failed to connect to {0}.

PAM-CMN-0414 = Invalid definition of virtual device {0}.

PAM-CMN-0415 = Physical device {0} may not have an alternate id.

PAM-CMN-0416 = Virtual device not available.

PAM-CMN-0417 = Target Application {0} was not added or updated due to Password Authority authorization errors.

PAM-CMN-0418 = Device group must have a provision type.

PAM-CMN-0419 = A device group's provision type may not be changed. Delete and recreate the group.

PAM-CMN-0420 = {0} device refresh failed due to error. See log for details.

PAM-CMN-0421 = Target server {0} not found.

PAM-CMN-0422 = Request server not found.

PAM-CMN-0423 = Special device {0} may not be changed.

PAM-CMN-0424 = Connection error - is DNS working? See log for details.

PAM-CMN-0425 = A target server with the address {0} already exists. Target server {1} not added.

PAM-CMN-0426 = A request server with the address {0} already exists. Request server {1} not added.

PAM-CMN-0427 = Invalid device type (access, password, a2a) specified.

PAM-CMN-0428 = {0} provisioning already in progress. Please wait.



PAM-CMN-0429 = Terminal type VT100 is not compatible with TN5250 or TN5250SSL access methods.

PAM-CMN-0430 = Device import cannot add VMware device groups only update them. Group name = {0}.

PAM-CMN-0431 = Could not reassign user to PA user.

PAM-CMN-0432 = General error with password checkin. See log for details.

PAM-CMN-0433 = {0} is a reserved {1} name. Please use another name.

PAM-CMN-0434 = {0} is a reserved device address. Please use another address.

PAM-CMN-0435 = Device may not have applets if not of typeAccess.

PAM-CMN-0436 = Device may not have services if not of typeAccess.

PAM-CMN-0437 = Target server fields may not be defined if device is not of typePassword.

PAM-CMN-0438 = Request server fields may not be defined if device is not of typeA2A.

PAM-CMN-0439 = Device import cannot add VMware Device Groups, it may only update them (Group name = {0}).

PAM-CMN-0440 = Configuring device {0} as a {1} device will exceed the number of licensed {2} devices. Device added without the type.

PAM-CMN-0441 = Internal error occurred while updating the runtime status of a device.

PAM-CMN-0442 = Service AWS Management Console SSO can not be added to a device.

PAM-CMN-0443 = {0} VMware devices were not deleted. See logs for details. VMware credentials are kept but the configuration is now inactive.

PAM-CMN-0444 = {0} AWS devices were not deleted. See logs for details. AWS credentials are kept but the configuration is now inactive.

PAM-CMN-0445 = AWS region code may not be changed on update. Delete this row and enter a new one.

PAM-CMN-0446 = AWS region code required.

PAM-CMN-0447 = Invalid AWS region code {0}.

PAM-CMN-0448 = This AWS access key and region are already provisioned.

PAM-CMN-0449 = The access key id must reference an actual Access Key target account.

PAM-CMN-0450 = The active checkbox must have a value of t or f.

PAM-CMN-0451 = Target application {0} from device {1} was not deleted.

PAM-CMN-0452 = Target application {0} was deleted from device {1}.

PAM-CMN-0453 = Service AWS API Proxy can not be added to a device.

PAM-CMN-0454 = Target group {0} not added to Password Authority. Error Message: {1}.

PAM-CMN-0455 = Unable to delete target group {0} from Password Authority. Error Message: {1}.

PAM-CMN-0456 = Request group {0} not added to Password Authority. Error Message: {1}.

PAM-CMN-0457 = Unable to delete request group {0} from Password Authority. Error Message: {1}.

PAM-CMN-0458 = AWS Proxy client authorization mapping failed. Error Message: {0}.

PAM-CMN-0459 = Deleting the AWS Proxy client authorization mapping failed. Error Message: {0}.

PAM-CMN-0460 = AWS Access key not found.

PAM-CMN-0461 = No such credential source as {0}. Device group {1} was added without it.

PAM-CMN-0462 = No such credential source as {0}. Device group {1} was updated, but the old credential was left in place.

PAM-CMN-0463 = Invalid value for password push flag.

PAM-CMN-0464 = {0} device group membership may not be changed locally. The {1} device groups were restored.

PAM-CMN-0465 = A target server with the device name {0} already exists. Target server not added.

PAM-CMN-0466 = A request server with the device name {0} already exists. Request server not added.

PAM-CMN-0467 = A Password Authority problem prevented completing the request. Message: {0} Check log for details.

PAM-CMN-0468 = The tag "{0}" has a length greater than {1}

PAM-CMN-0469 = Command {0} not supported for transparent login. Only the commands {1} are supported.

PAM-CMN-0470 = Password prompt for {0} command may not contain equals sign or semi-colon.

PAM-CMN-0471 = Password prompt is required for transparent login.

PAM-CMN-0472 = Full path must begin with a forward slash (/).

PAM-CMN-0473 = Must specify both full path and prompt or neither.

PAM-CMN-0474 = The same user may not be assigned twice to the same vCenter for provisioning.

PAM-CMN-0475 = Target account id is required for update of target account {0}.

PAM-CMN-0476 = Either the hostname and the target application application name, or the target application id is required to add the target account {0}.

PAM-CMN-0477 = Target account id and user name are both required to update a target account.

PAM-CMN-0478 = VMware URL most commonly should be in the form https://<domain>[:port]/sdk. Please enter a URL.

PAM-CMN-0479 = Provision id required.

PAM-CMN-0480 = Only the url or the active status may be changed, and one of them must be changed on an update.

PAM-CMN-0481 = Device must be at least of type Access, Password, or A2A.

PAM-CMN-0482 = Invalid device group ids specified. The array must contain only numeric ids.

PAM-CMN-0483 = The following ids are not ids of existing device groups: {0}.

PAM-CMN-0484 = Invalid device service ids specified. The array must contain only numeric ids.

PAM-CMN-0485 = The following ids are not ids of valid TCP/UDP or RDP application services: {0}.

PAM-CMN-0486 = Invalid device VPN service ids specified. The array must contain only numeric ids.

PAM-CMN-0487 = The following ids are not ids of valid VPN services: {0}.

PAM-CMN-0488 = The following ids are not ids of valid TCP/UDP services: {0}.

PAM-CMN-0489 = The following ids are not ids of valid RDP application services: {0}.

PAM-CMN-0490 = Invalid device credential source ids specified. The array must contain only numeric ids.

PAM-CMN-0491 = The following ids are not ids of valid password devices: {0}.

PAM-CMN-0492 = Invalid device group service ids specified. The array must contain only numeric ids.

PAM-CMN-0493 = Invalid device group VPN service ids specified. The array must contain only numeric ids.

PAM-CMN-0494 = Invalid device ids specified. The array must contain only numeric ids.

PAM-CMN-0495 = The following ids are not ids of existing devices: {0}.

PAM-CMN-0496 = Target application {0} was not found.

PAM-CMN-0497 = X11 Forwarding can only be applied to the SSH applet.

PAM-CMN-0498 = Only X11 Forwarding (x11forwarding) is a valid task property.

PAM-CMN-0499 = A virtual device may not be added via local means.

PAM-CMN-0500 = Device name and domain name of a virtual device may not be changed via local means.

PAM-CMN-0501 = Virtual device {0} may not be deleted via local means.

PAM-CMN-0502 = Special device {0} may not be deleted.

PAM-CMN-0503 = Device was not found.

PAM-CMN-0504 = The specified device is not a password type device.

PAM-CMN-0505 = A target application with the specified id was not found or does not belong to the specified device.

PAM-CMN-0506 = Target account not found.

PAM-CMN-0507 = Device was not found or was not a target server.

PAM-CMN-0508 = Target application does not belong to device.

PAM-CMN-0509 = A target application with the same name already exists for the device.

PAM-CMN-0510 = Invalid target application type specified. Valid types are: Generic, UnixII.

PAM-CMN-0511 = Error occurred provisioning the target account.

PAM-CMN-0512 = A target account with the specified id was not found or does not belong to the specified device or target application.

PAM-CMN-0513 = Error occurred updating the target account.

PAM-CMN-0514 = Tags must be an array of tag names.

PAM-CMN-0515 = The device already has the following {0} services: {1}.

PAM-CMN-0516 = Tag id must be an integer.

PAM-CMN-0517 = Transparent login parameters must be in the form command;prompt|command;prompt. Semicolon, comma, and pipe may not be used as part of the command or the prompt.

PAM-CMN-0518 = Invalid transparent login type.

PAM-CMN-0519 = Transparent login type and parameters out of sync.

PAM-CMN-0520 = Secondary SSO must be defined as <Device Name>|<TargetApplication Name>|<TargetAccount user name>.

PAM-CMN-0521 = Failed to assign '{0}' tag to device. '{1}' tag prefix is reserved for vSphere NSX Security {2}.

PAM-CMN-0522 = Service VMware NSX API Proxy can not be added to a device.

PAM-CMN-0523 = NSX Proxy is a reserved {0} name. Please use another name.

PAM-CMN-0524 = [ca.nsx.vmware.com](https://ca.nsx.vmware.com) is a reserved device address. Please use another address.

PAM-CMN-0525 = Tags may not be defined on non-local groups.

PAM-CMN-0526 = Invalid value for Override Address.

PAM-CMN-0527 = Cannot delete Password Management device {0} because it is configured as a VMware vCenter device for CA PAM.

PAM-CMN-0528 = Command string {0} begins with a forward slash (/), which is not allowed in transparent login command strings.

PAM-CMN-0529 = Invalid value for Handle Legal Notice flag.

PAM-CMN-0530 = Cannot get name for a target or request group if no group ID is supplied.

PAM-CMN-0531 = Device {0} had missing terminal data; default terminal data has been assigned.

PAM-CMN-0532 = Device name {0} was successfully managed.

PAM-CMN-0533 = {0} device(s) not deleted because they are in use.

PAM-CMN-0534 = Device Manager user couldn't delete device {0} because it is a Password Management or A2A device and the user lacks privileges to delete those types of device.

PAM-CMN-0535 = Device Manager user couldn't change name of device {0} because it is a Password Management or A2A device and the user lacks privileges to rename those types of device.

PAM-CMN-0536 = Device Manager user couldn't change domain name of device {0} because it is a Password Management or A2A device and the user lacks privileges to change domain names for those types of device.

PAM-CMN-0537 = Role was not found.

## Role and Privilege Messages

PAM-CMN-0538 = Update of role {0} failed. No matching id.

PAM-CMN-0539 = Role requested to be assigned a non-existent privilege.

PAM-CMN-0540 = Role id must be an integer, not {0}.

PAM-CMN-0541 = Default roles may not be deleted or updated.

PAM-CMN-0542 = Role not found to {0}.

PAM-CMN-0543 = Role not deleted because there are still users assigned to it.

PAM-CMN-0544 = Role id required when updating a role.

PAM-CMN-0545 = Role id already assigned at start of add. Role was not added.

PAM-CMN-0546 = Duplicate role name {0}.

PAM-CMN-0547 = Create role failed for role {0}.

PAM-CMN-0548 = Role name may not be changed.

PAM-CMN-0549 = Role {0} missing required {1}.

PAM-CMN-0550 = Role {0} with these groups may not be added to a user by this user.

PAM-CMN-0551 = Role {0} may not have its {1} changed by this user.

PAM-CMN-0552 = The Autodiscovery role requires Device/Group Manager role or the Delegated Administrator Role as well.

PAM-CMN-0553 = A role must contain at least one privilege.

PAM-CMN-0554 = Due to role restrictions, group {0} may not be added to a user except by a Global Administrator.

PAM-CMN-0555 = Roles containing the AWS API Proxy privilege may not be added to groups.

PAM-CMN-0556 = Role with id {0} not found.

PAM-CMN-0557 = The following user groups for role {0} do not exist: {1}.

PAM-CMN-0558 = The following device groups for role {0} do not exist: {1}.

PAM-CMN-0559 = The API key {0} for user {1} has privileges the user does not. The API key will be disabled until this is fixed.

## Device Group Management Messages

PAM-CMN-0560 = Device group name is required.

PAM-CMN-0561 = Invalid device group name specified.

PAM-CMN-0562 = Invalid device group description specified.

PAM-CMN-0563 = Invalid device group id specified.

PAM-CMN-0564 = Device group name {0} already exists.



PAM-CMN-0565 = Device group with name {0} not found.  
PAM-CMN-0566 = Device group with id {0} not found.  
PAM-CMN-0567 = {0} field must be an array.  
PAM-CMN-0568 = Device group {0} not inserted.  
PAM-CMN-0569 = Database corruption - more than one device group with the same id was inserted.  
PAM-CMN-0570 = Device group {0} not updated.  
PAM-CMN-0571 = Database corruption - more than one device group with the same id was updated.  
PAM-CMN-0572 = Device group {0} not deleted.  
PAM-CMN-0573 = Database corruption - more than one device group with the same id was deleted.  
PAM-CMN-0574 = {0} device group(s) deleted.  
PAM-CMN-0575 = {0} device group(s) deleted, {1} user group(s) not deleted.  
PAM-CMN-0576 = Device group cannot have both sftpftp and sftpftpemb services.  
PAM-CMN-0577 = {0} device group(s) not deleted because not authorized.  
PAM-CMN-0578 = {0} device group(s) not deleted because not found.  
PAM-CMN-0579 = {0} device group(s) not deleted because of unknown error.  
PAM-CMN-0580 = {0} device group(s) deleted. {0} {1} {2}  
PAM-CMN-0581 = Device group cannot have both sftpsftp and sftpsftpemb services.  
PAM-CMN-0582 = A device group with a network address cannot have services or access methods defined.  
PAM-CMN-0583 = Invalid network address {0}.  
PAM-CMN-0584 = The following device groups do not exist: {0}.  
PAM-CMN-0585 = VMware device group {0} may not be deleted locally.  
PAM-CMN-0586 = Device group not found.  
PAM-CMN-0587 = The device group already has the following access methods: {0}.  
PAM-CMN-0588 = The device group already has the following {0} services: {1}.  
PAM-CMN-0589 = The specified access method id does not belong to the device group or is invalid.  
PAM-CMN-0590 = The specified service id does not belong to the device group or is invalid.  
PAM-CMN-0591 = The specified VPN service id does not belong to the device group or is invalid.

## Global Settings and Device Task Messages

PAM-CMN-0592 = Task name or id is required.  
PAM-CMN-0593 = Invalid task port specified.  
PAM-CMN-0594 = Task enabled is required.  
PAM-CMN-0595 = Invalid task enabled specified.  
PAM-CMN-0596 = Invalid task id specified.  
PAM-CMN-0597 = Task not found.  
PAM-CMN-0598 = Invalid task name specified.  
PAM-CMN-0599 = Device group contains invalid task name(s): {0}.  
PAM-CMN-0600 = Device group contains invalid service name(s): {0}.  
PAM-CMN-0601 = Device group contains invalid SSL VPN service name(s): {0}.  
PAM-CMN-0602 = Device group contains invalid device name(s): {0}.  
PAM-CMN-0603 = Device group cannot contain other device groups: {0}.  
PAM-CMN-0604 = Access method may not be defined twice on the same device.  
PAM-CMN-0605 = Invalid access method type(s) {0}.

## LDAP Messages

PAM-CMN-0606 = LDAP entry must be of type UserGroupType to retrieve group users.

PAM-CMN-0607 = LDAP user group does not contain any users.

PAM-CMN-0608 = LDAP connection failure: {0}.

PAM-CMN-0609 = LDAP bind failure: {0}.

PAM-CMN-0610 = LDAP query failure: {0}.

PAM-CMN-0611 = Starting point for browsing LDAP directory is not under configured browse points.

PAM-CMN-0612 = LDAP domain not found.

PAM-CMN-0613 = LDAP update in progress, please try again later.

PAM-CMN-0614 = LDAP Group {0} imported into CA PAM. {1} Users Processed: {2} New Users, {3} Updated Users, {4} Deleted Users, {5} Failed New Users, {6} Failed Updated Users, {7} Failed Deleted Users.

PAM-CMN-0615 = LDAP import failed: {0}

PAM-CMN-0616 = {0} LDAP group(s) completed with errors. Please check the audit log on the cluster master for more details.

PAM-CMN-0617 = There are no imported LDAP groups to refresh.

PAM-CMN-0618 = Warning: user {0} from LDAP group {1} has same short name, {2}, as user {3} from LDAP group {4}. RADIUS authentication process will not be able to differentiate between the two users. Both user accounts will be deactivated.

PAM-CMN-0619 = Unauthorized attempt to retrieve the configuration for LDAP domains.

PAM-CMN-0620 = Connection failed to LDAP domain {0} using server {1}. Failing over to the next configured LDAP server.

PAM-CMN-0621 = Import Warning For LDAP Group {0}: {1}

PAM-CMN-0622 = Import Error For LDAP Group {0}: {1}

PAM-CMN-0623 = Invalid LDAP group(s) specified: {0}.

PAM-CMN-0624 = LDAP Group {0} imported into CA PAM. {1} Devices Processed: {2} New Devices, {3} Updated Devices, {4} Deleted Devices, {5} Failed New Devices, {6} Failed Updated Devices, {7} Failed Deleted Devices.

PAM-CMN-0625 = Adding LDAP group {0} aborted. The LDAP group and all its registered members will be deleted.

PAM-CMN-0626 = STARTTLS LDAP connection made to {0}.

PAM-CMN-0627 = LDAP connection made to {0}.

PAM-CMN-0628 = An LDAP operation is in progress.

PAM-CMN-0629 = LDAPS connection made to {0}.

PAM-CMN-0630 = LDAP is configured but the appliance is unlicensed. License the appliance before launching the LDAP browser.

PAM-CMN-1932 = "Invalid LDAP Domain Id {0}"

PAM-CMN-5405 = "Unable to delete user, because it is configured for Forced Deactivation Alert."

## CSV Import/Export Related Messages

PAM-CMN-0631 = Invalid file type of {0}. Import supports only CSV files of types: {1}.

PAM-CMN-0632 = Import file cannot be found.

PAM-CMN-0633 = Invalid CSV row type {0} on line {1}.

PAM-CMN-0634 = Error importing user on line {0}:

PAM-CMN-0635 = User group {0} does not exist.

PAM-CMN-0636 = Role {0}, does not exist: {1}.

PAM-CMN-0637 = Role user group, {0}, does not exist: {1}.

PAM-CMN-0638 = Role device group, {0}, does not exist: {1}.

PAM-CMN-0639 = Invalid import file. CSV headers are missing.

PAM-CMN-0640 = Unrecognized CSV header: {0}.

PAM-CMN-0641 = Number of CSV data fields ({0}) does not match CSV header count ({1}) on line {2}.

PAM-CMN-0642 = First CSV header must be Type.

PAM-CMN-0643 = User created successfully.

PAM-CMN-0644 = User updated successfully.

PAM-CMN-0645 = User Group created successfully.

PAM-CMN-0646 = User Group updated successfully.

PAM-CMN-0647 = Error occurred during import.

PAM-CMN-0648 = Device Group {0} does not exist.

PAM-CMN-0649 = Device created successfully.

PAM-CMN-0650 = Device updated successfully.

PAM-CMN-0651 = Device Group created successfully.

PAM-CMN-0652 = Device Group updated successfully.

PAM-CMN-0653 = Invalid task name specified: {0}.

PAM-CMN-0654 = Console device {0} does not exist.

PAM-CMN-0655 = Power device {0} does not exist: {1}.

PAM-CMN-0656 = Device access method types do not exist: {0}.

PAM-CMN-0657 = Device services do not exist: {0}.

PAM-CMN-0658 = TCP/UDP services with both TCP and UDP ports defined must have the same port value(s).

PAM-CMN-0659 = Service created successfully.

PAM-CMN-0660 = Service updated successfully.

PAM-CMN-0661 = Invalid role privileges: {0}.

PAM-CMN-0662 = Role created successfully.

PAM-CMN-0663 = Role updated successfully.

PAM-CMN-0664 = Policy created successfully.

PAM-CMN-0665 = Policy updated successfully.

PAM-CMN-0666 = Device {0} does not have access method {1}.

PAM-CMN-0667 = Device {0} does not have access method {1}, with name {2}.

PAM-CMN-0668 = Device {0} does not have service {1}.

PAM-CMN-0669 = Device {0} does not have VPN service {1}.

PAM-CMN-0670 = Invalid {0} value. Valid values are: t, f.

PAM-CMN-0671 = Socket filter list entry created successfully.

PAM-CMN-0672 = Socket filter list entry updated successfully.

PAM-CMN-0673 = Command filter list entry created successfully.

PAM-CMN-0674 = Command filter list entry updated successfully.

PAM-CMN-0675 = Import failed: CSV file not specified.

PAM-CMN-0676 = Device {0} does not have target application {1}.

PAM-CMN-0677 = Device {0} does not have target account {1}.

PAM-CMN-0678 = Target account {0} does not have the correct id.

PAM-CMN-0679 = Socket filter list entry already exists and therefore will not be added.

PAM-CMN-0680 = Import failed: SAML metadata file not specified.

PAM-CMN-0681 = The policy for the specified SAML Service Policy doesn't exist. Provision the policy before importing the SAML Service.

PAM-CMN-0682 = The SAML service {0} doesn't exist.

PAM-CMN-0683 = The specified SAML service has not been assigned to the device.

PAM-CMN-0684 = CSV import of type {0} initiated.

PAM-CMN-0685 = Device Group {0} does not have credential source {1}.

## Office365 Integration Messages, SAML IdP and SP Messages

PAM-CMN-0686 = Default default contact user {0} does not exist.

PAM-CMN-0687 = Invalid default contact method {0} specified.

PAM-CMN-0688 = Device monitor protocol required.

PAM-CMN-0689 = Device monitor port required for protocol {0}.

PAM-CMN-0690 = Device monitor contact required for protocol {0}.

PAM-CMN-0691 = Device monitor contact method required for protocol {0}.

PAM-CMN-0692 = Invalid device monitor protocol specified.

PAM-CMN-0693 = Invalid device monitor port {0} specified for protocol {1}.

PAM-CMN-0694 = Invalid device contact method specified for protocol {0}.

PAM-CMN-0695 = Device monitor contact {0} does not exist.

PAM-CMN-0696 = Maximum buffer size is 8192.

PAM-CMN-0697 = Invalid web session recording quality specified. Valid values are high and low.

PAM-CMN-0698 = Unauthorized attempt to delete policies associated with the Office365 service.

PAM-CMN-0699 = Calculating the certificate fingerprint for IdP {0} failed. The IdP configuration will not be saved.

PAM-CMN-0700 = The SAML SP's {0} is a required field. Please enter a valid value.

PAM-CMN-0701 = The SAML SP's Fully Qualified Hostname is not a valid hostname.

PAM-CMN-0702 = The {0} of Identity Provider {1} is a required field. Please enter a valid value.

PAM-CMN-0703 = Invalid Identity Provider SSO binding specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0704 = The Single Sign On Service URL for Identity Provider {0} is not a valid HTTP URL.

PAM-CMN-0705 = The specified {0} of Identity Provider {1} is invalid. Valid values are: true or false.

PAM-CMN-0706 = The specified certificate for Identity Provider {0} is not a valid PEM certificate.

PAM-CMN-0707 = Invalid Signature Algorithm specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0708 = Invalid Name ID Formats specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0709 = Invalid Authentication Contexts specified for Identity Provider {0}. Valid values are: {1}.

PAM-CMN-0710 = Identity Provider entity IDs must be unique. There are multiple identity providers with the following entity ID(s): {0}.

PAM-CMN-0711 = Invalid SAML version specified for Identity Provider {0}. Valid values are: 1.1, 2.0

PAM-CMN-0712 = CA PAM as SAML SP configuration updated.

PAM-CMN-0713 = Identity Provider friendly names must be unique. There are multiple identity providers with the following friendly name(s): {0}.

PAM-CMN-0714 = Invalid vulnerability reporting level specified. Valid values are 'Log' or 'Log And Warn'.

PAM-CMN-0715 = Invalid vulnerability enabled specified.

PAM-CMN-0716 = The following required fields in the SAML SP configuration must be specified before the configuration can be saved or an IdP can be configured: Entity ID, Fully Qualified Hostname, Certificate Key Pair.

PAM-CMN-0717 = The required field, 'Fully Qualified Hostname', in the SAML configuration on cluster member {0} has not been defined. Please specify a value for the field before downloading metadata.

PAM-CMN-0718 = SAML SP metadata for remote IdP {0} downloaded.

PAM-CMN-0719 = An attempt was made to access the SAML IdP Proxy service when CA PAM is not deployed in a cluster.

PAM-CMN-0720 = An error occurred while completing this request. Please contact your administrator for further assistance.

PAM-CMN-0721 = An attempt was made to access the SAML IdP Proxy service on this node but this node is not the cluster master.

PAM-CMN-0722 = The following remote IdP(s) have been deleted: {0}.

PAM-CMN-0723 = The following remote IdP(s) have been added: {0}.

PAM-CMN-0724 = The id of identity provider {0} is not a valid id: {1}.

PAM-CMN-0725 = Invalid value specified ({0}). Integer expected.

PAM-CMN-0726 = Invalid value specified for SAML Accept RSA-SHA1 Signed Responses. Valid values are: t,f.

PAM-CMN-0727 = Invalid value specified for Client Distribution Intranet URL. Only domain names and IP addresses are allowed.

PAM-CMN-0728 = Invalid port specified for Client Distribution Intranet URL.

PAM-CMN-1818 = No user name supplied for Office 365.

PAM-CMN-1921 = Updated Microsoft Office 365 configuration

PAM-CMN-1922 = Cleared Microsoft Office 365 configuration

PAM-CMN-1923 = Office 365 configuration test: Connected successfully to the supplied URLs

PAM-CMN-1924 = Office 365 configuration test: Error connecting to the supplied URLs

PAM-CMN-2346 = Updated Microsoft Office 365 configuration

PAM-CMN-2347 = Cleared Microsoft Office 365 configuration

PAM-CMN-2348 = Office 365 configuration test: Connected successfully to the supplied URLs

PAM-CMN-2349 = Office 365 configuration test: Error connecting to the supplied URLs

## Policy Management Messages

PAM-CMN-0729 = Unexpected from location for policy request of {0}.

PAM-CMN-0730 = Invalid service specified in policy.

PAM-CMN-0731 = Invalid task specified in policy.

PAM-CMN-0732 = Invalid socket filter specified in policy.

PAM-CMN-0733 = Invalid command filter specified in policy.

PAM-CMN-0734 = Invalid CLI session recording flag in policy.

PAM-CMN-0735 = Invalid graphical session recording flag in policy.

PAM-CMN-0736 = Invalid bidirectional flag in policy.

PAM-CMN-0737 = Invalid VPN service specified in policy.

PAM-CMN-0738 = Invalid restrict login if agent is not running value. Valid values are: t, f.

PAM-CMN-0739 = AWS Policy can be specified only for AWS service.

PAM-CMN-0740 = Unable to display credentials. See log for details.

PAM-CMN-0741 = Web portal recording can only be enabled for policies that contain a web portal services utilizing the CA browser. Please set the browser type property of the service to CA.

PAM-CMN-0742 = Policies involving [ca.aws.amazon.com](https://ca.aws.amazon.com) may not be imported or exported via csv.

PAM-CMN-0743 = Attempt to add a target account {0} to a policy that does not have access to it.

PAM-CMN-0744 = There is credentials conflict in Transparent Login Window with title '{0}' ('{1}' and '{2}' RDP Applications).

PAM-CMN-0745 = The policy data structure specified is invalid. {0}.

PAM-CMN-0746 = The policy's device does not offer any access methods for policy. Please add access methods to the device first.

PAM-CMN-0747 = The policy's device does not offer device access methods with the following id(s): {0}.

PAM-CMN-0748 = The policy's device does not offer any TCP/UDP nor RDP application services for policy. Please add services to the device first.

PAM-CMN-0749 = The policy's device does not offer TCP/UDP nor RDP application services with the following id(s): {0}.

PAM-CMN-0750 = The policy's device does not offer any VPN services for policy. Please add VPN services to the device first.

PAM-CMN-0751 = The policy's device does not offer VPN services with the following id(s): {0}.

PAM-CMN-0752 = The specified target account id is invalid: {0}.



PAM-CMN-0753 = The restrict login flag requires a socket filter list to be set for this policy.

PAM-CMN-0754 = No applets or services which support CLI recording are selected.

PAM-CMN-0755 = No applets or services which support graphical recording are selected.

PAM-CMN-0756 = No applets or services which support bidirectional CLI recording are selected.

PAM-CMN-0757 = The specified device does not offer any target accounts for viewing. Please add target accounts to the device first.

PAM-CMN-0758 = A policy must specify either an access method, a service, a vpn service, or target accounts.

PAM-CMN-0759 = The bidirectional flag may only be set on if CLI recording is selected.

PAM-CMN-0760 = Transparent login not defined for any selected access method or service.

PAM-CMN-0761 = A policy association between user (group) {0} and device (group) {1} doesn't exist.

PAM-CMN-0762 = No such policy exists.

PAM-CMN-0763 = The specified user or user group id was not found.

PAM-CMN-0764 = The specified device or device group id was not found.

PAM-CMN-0765 = The specified account id is not selected in the policy for viewing.

PAM-CMN-0766 = The policy does not contain the access method with id {0}. Use POST for adding.

PAM-CMN-0767 = The policy already contains the access method with id {0}. Use PUT for updates.

PAM-CMN-0768 = The policy does not contain the service with id {0}. Use POST for adding.

PAM-CMN-0769 = The policy already contains the service with id {0}. Use PUT for updates.

PAM-CMN-0770 = The policy already contains the SSLVPN service with id {0}.

PAM-CMN-0771 = The policy is already configured to allow viewing the password for the account with id {0}.

PAM-CMN-0772 = The following account id(s) do not belong to the specified device: {0}.

PAM-CMN-0773 = A policy association between the specified user (group) and device (group) already exists.

PAM-CMN-0774 = A mapping for the required SAML attribute, {0}, for users with provision type {1} must be defined.

PAM-CMN-0775 = The following SAML attributes have not been mapped to a valid value: {0}.

PAM-CMN-0776 = The following provision types have multiple Subject Name Identifier mappings defined: {0}. There can only be one mapping defined per provision type.

PAM-CMN-0777 = The following SAML requested attribute ids for SAML resolved attributes are invalid: {0}.

PAM-CMN-0778 = The format for the following SAML attribute is invalid: {0}. Expected format is: {1}.

PAM-CMN-0779 = Requested SAML attribute with name {0} doesn't exist.

PAM-CMN-0780 = Target servers and all associated applications and accounts were deleted from policies.

PAM-CMN-0781 = Target applications and all associated accounts were deleted from policies.

PAM-CMN-0782 = Target accounts were deleted from policies.

PAM-CMN-0783 = Target account belonging to device {0} for target application {1} with user name {2} not found.

PAM-CMN-0784 = Policies involving [ca.nsx.vmware.com](https://ca.nsx.vmware.com) may not be imported or exported via csv.

PAM-CMN-0785 = AWS Policy value is not specified for AWS service.

PAM-CMN-0786 = ssoWindow winId {0} is not valid for RDP Application service id {1}. Either the winId doesn't exist or it is not assigned to the service.

PAM-CMN-0787 = Invalid account triplet specified: {0}.

## Management Console Messages

PAM-CMN-0788 = Invalid policy name specified. Policy name must be alpha-numeric.

PAM-CMN-0789 = Policy name required.

PAM-CMN-0790 = Invalid policy version specified.

PAM-CMN-0791 = Invalid policy description specified.

PAM-CMN-0792 = CA PAM appliance already imported into management console.

PAM-CMN-0793 = Working set with the specified name already exists.

PAM-CMN-0794 = Invalid policy module specified.

PAM-CMN-0795 = A policy must contain at least one module before associating it with an CA PAM appliance.

PAM-CMN-0796 = Unable to successfully authenticate to server {0}.

PAM-CMN-0797 = Invalid policy specified.

PAM-CMN-0798 = CA PAM credentials not specified. Please set the credentials for the server or set the default credentials for all servers.

PAM-CMN-0799 = Unable to establish connection to CA PAM appliance {0}.

### **Management Console API Messages**

PAM-CMN-4800 = External API License is required for Management Console licensing.

PAM-CMN-4801 = Once an appliance is a management console it may never revert to an ordinary PAM appliance.

PAM-CMN-4802 = Invalid value for PAM Management Console.

PAM-CMN-4803 = Internal user for collecting data for PAM Management Console.

PAM-CMN-4804 = API key for collecting data for PAM Management Console.

PAM-CMN-4805 = Successfully created internal user {0} for PAM Management Console.

PAM-CMN-4806 = Failed to properly initialize PAM Management Console.

PAM-CMN-4807 = Allows read only access to the PAM Management Console.

PAM-CMN-4808 = Allows create and update access to the PAM Management Console.

PAM-CMN-4809 = Allows access to PAM Management Console Administration UI.

PAM-CMN-4810 = Failed to define proper password for MCApiUser's API key.

PAM-CMN-4811 = Allows the user to view the PAM Management Console.

PAM-CMN-4812 = Allows the user to change the PAM Management Console.

PAM-CMN-4813 = Allows the user to access the PAM Management Console Administration UI.

PAM-CMN-4814 = The PAM Management Console API user may not have its roles changed.

PAM-CMN-4815 = The PAM Management Console API user may not be deleted.

PAM-CMN-4850 = User defined roles may not contain the Global Administrator privilege nor any PAM Management Console related privilege.

### **Managed Server Service Messages**

PAM-CMN-0800 = CA PAM appliance is already being managed by a management console.

PAM-CMN-0801 = Apply policy {0} failed.

### **Command and Socket Filter Messages**

PAM-CMN-0802 = Violations before action value must be a positive number.

PAM-CMN-0803 = Violations before action value must be greater than 0.

PAM-CMN-0804 = Invalid intervention action specified.

PAM-CMN-0805 = Invalid agent listening port. Port must be a valid TCP port.

PAM-CMN-0806 = Invalid CA PAM appliance ID. ID must be numeric and between 1 and 254.

PAM-CMN-0807 = SFA Monitoring is required.

PAM-CMN-0808 = Socket filter list name required.

PAM-CMN-0809 = Socket filter list type required.

PAM-CMN-0810 = Invalid characters in socket filter list name. Semicolons, commas, percent signs, and backslashes are invalid.

PAM-CMN-0811 = Invalid socket filter list type. Valid types are: black, white.

PAM-CMN-0812 = Socket filter host address required.

PAM-CMN-0813 = Invalid socket filter host address. Address must be a valid IP address.

PAM-CMN-0814 = Socket filter port required.

PAM-CMN-0815 = Invalid socket filter port {0}. Port must be a valid TCP port.

PAM-CMN-0816 = A socket filter list with name {0} already exists.

PAM-CMN-0817 = Socket filter list not found.

PAM-CMN-0818 = Command filter list name required.

PAM-CMN-0819 = Command filter list type required.

PAM-CMN-0820 = Invalid characters in command filter list name. Semicolons, commas, percent signs, and backslashes are invalid.

PAM-CMN-0821 = Invalid command filter list type. Valid types are: black, white.

PAM-CMN-0822 = Invalid command filter alert value. Valid values are: t, f.

PAM-CMN-0823 = Invalid command filter block value. Valid values are: t, f.

PAM-CMN-0824 = Invalid command filter regular expression value. Valid values are: t, f.

PAM-CMN-0825 = Command filter keyword required.

PAM-CMN-0826 = A command filter list with name {0} already exists.

PAM-CMN-0827 = Socket filter list id must be a positive integer.

PAM-CMN-0828 = Command filter list id must be a positive integer.

PAM-CMN-0829 = Command filter list not found.

PAM-CMN-0830 = Duplicate entry, {0}, defined for socket filter list.

PAM-CMN-0831 = Duplicate keyword, {0}, defined for command filter list.

PAM-CMN-0832 = Duplicate ports {0} for socket filter host {1}.

PAM-CMN-0833 = SFA Log All Access value required.

PAM-CMN-0834 = Either (comma delimited) individual ports or a single port range must be specified, not ({0}).

PAM-CMN-0835 = A comma delimited port string cannot be more than 512 characters long.

PAM-CMN-0836 = Invalid AWS policy name {0}. Name must only have alphanumeric characters and =, . @ or -.

PAM-CMN-0837 = AWS policy not found.

PAM-CMN-0838 = AWS policy name cannot be longer than 128 characters.

PAM-CMN-0839 = AWS policy name {0} must be unique.

PAM-CMN-0840 = AWS policy is in use and may not be deleted.

PAM-CMN-0841 = AWS session duration invalid.

PAM-CMN-0842 = JSON for AWS policy invalid.

PAM-CMN-0843 = AWS policy too large to compile. See log for details.

PAM-CMN-0844 = AWS policy invalid. See log for details.

PAM-CMN-0845 = AWS policy required.

PAM-CMN-0846 = In order to create an AWS policy at least one Access Key must be defined in Password Authority.

PAM-CMN-0847 = Invalid filter list type specified. Valid values are: white, black.

PAM-CMN-0848 = The enabled filter is not supported for SSLVPN service type.

PAM-CMN-0849 = The command filter {0} has been deleted.

PAM-CMN-0850 = The socket filter {0} has been deleted.

## Logging and Reporting Messages

PAM-CMN-0851 = Cannot add an existing report.

PAM-CMN-0852 = Report name required.

PAM-CMN-0853 = Choose either relative or absolute date range.

PAM-CMN-0854 = Badly formed relative date interval.

PAM-CMN-0855 = Invalid relative date reporting interval.

PAM-CMN-0856 = Invalid relative date reporting amount.

PAM-CMN-0857 = At least one column must be specified for a report.

PAM-CMN-0858 = Invalid email address specified. Multiple addresses must be separated by a comma.

PAM-CMN-0859 = Email address required.

PAM-CMN-0860 = The interval between emails is not defined properly.

PAM-CMN-0861 = The time to send the email is not defined properly.

PAM-CMN-0862 = Email send interval required.

PAM-CMN-0863 = Only the original author of a report or a Global Administrator may update or delete it.

PAM-CMN-0864 = Relative report dates must specify the number of days, weeks or months to include in the report.

PAM-CMN-0865 = Log report not found.

PAM-CMN-0866 = Invalid date range format.



PAM-CMN-0867 = Start date must be before end date.  
 PAM-CMN-0868 = Invalid list of columns for report.  
 PAM-CMN-0869 = Unable to locate recording data. The file may have been removed, or the mount may be down.  
 PAM-CMN-0870 = Session Recording Integrity Failure: This session recording appears to have been modified since it was recorded. Proceed at your own risk.  
 PAM-CMN-0871 = A report named {0} already exists for this user.  
 PAM-CMN-0872 = startDate must be specified if endDate is specified.  
 PAM-CMN-0873 = endDate must be specified if startDate is specified.  
 PAM-CMN-0874 = Session recording can not be started for '{0}' in {1} safe mode because mount is down.  
 PAM-CMN-0875 = Session recording can not be started for '{0}' because {1} session recording is disabled.  
 PAM-CMN-0876 = Network mount for session recording unavailable.  
 PAM-CMN-0877 = Invalid format of Start Date.  
 PAM-CMN-0878 = Invalid format of End Date.  
 PAM-CMN-0879 = Invalid selected range type format.  
 PAM-CMN-0880 = Email daily time required.  
 PAM-CMN-1080 = Unauthorized attempt to add a message to the audit log: {0}  
 PAM-CMN-1371 = Log records viewed

#### NOTE

The PAM-CMN-1371 message appears twice when someone logs into the CA PAM UI. This is expected behavior as the UI queries the log to obtain information to appear under **Recent Events** and to populate the **Dashboard Overview Tab**.

PAM-CMN-1372 = Downloaded log records  
 PAM-CMN-1373 = Failed to update status of log row {0}  
 PAM-CMN-1374 = Log report {0} successfully added  
 PAM-CMN-1375 = Log report {0} not added  
 PAM-CMN-1376 = Log report {0} updated  
 PAM-CMN-1377 = Update of log report {0} failed  
 PAM-CMN-1378 = Log report {0} was deleted  
 PAM-CMN-1379 = Log report {0} was not deleted  
 PAM-CMN-1490 = Unable to purge the logs! Please, contact your administrator!  
 PAM-CMN-1491 = All logs have been purged!  
 PAM-CMN-1492 = Log file {0} deleted successfully  
 PAM-CMN-1493 = Unable to delete log file {0}  
 PAM-CMN-1494 = Changed automatic Log Purge Settings. Status: Enabled, Purge interval: {0} Hour(s), Email flag: {1} Email size: {2}MB  
 PAM-CMN-1495 = Changed automatic Log Purge Settings. Status: Disabled  
 PAM-CMN-1496 = External Log Settings saved successfully.  
 PAM-CMN-1497 = Cannot create log table on the external server.  
 PAM-CMN-1498 = Created new log table on the external server.  
 PAM-CMN-1499 = Cannot create log\_user\_group table on the external server.  
 PAM-CMN-1500 = Created new log\_user\_group table on the external server.  
 PAM-CMN-1501 = Cannot create log\_device\_group table on the external server.  
 PAM-CMN-1502 = Created new log\_device\_group table on the external server.  
 PAM-CMN-1920 = Downloaded log file {0}.  
 PAM-CMN-2008 = logwatch[{0}]: "mail error: {1}"  
 PAM-CMN-2009 = logwatch[{0}]: "Log id {1} to {2} deleted, no mail sent."  
 PAM-CMN-2010 = logwatch[{0}]: "Log id {1} to {2} deleted, mail sent OK."  
 PAM-CMN-2011 = logwatch[{0}]: "Log id {1} to {2} deleted, mail error: {3}"  
 PAM-CMN-2012 = logwatch[{0}]: "Problem deleting log id {1} to {2}, no mail sent."

PAM-CMN-2013 = logwatch[{0}]: "Problem deleting log id {1} to {2}, mail sent OK."

PAM-CMN-2014 = logwatch[{0}]: "Problem deleting log id {1} to {2}, mail error: {3}"

PAM-CMN-2015 = logwatch[{0}]: "Starting up logwatch"

PAM-CMN-2345 = Downloaded log file {0}.

PAM-CMN-2590 = Not connected to the external log server.

PAM-CMN-2591 = No logs to send.

PAM-CMN-2603 = No log files exist!

PAM-CMN-3136 = Metrics auto archive failed. Please check Settings, Credential Manager Settings, Auto-Archive.

PAM-CMN-3137 = Audit Log auto archive failed. Please check Settings, Credential Manager Settings, Auto-Archive.

## Policy Conflict Messages

PAM-CMN-0881 = Updating the group membership for {0} will cause a {1} filter policy conflict for {2} from the following policies:

PAM-CMN-0882 = Socket filter {0} list policy {1} from association between user {2} and device {3}.

PAM-CMN-0883 = Command filter {0} list policy {1} from association between user {2} and device {3}.

PAM-CMN-0884 = Adding {0} to group {1} will cause a {2} filter policy conflict for {3} from the following policies:

PAM-CMN-0885 = Adding device {0} to {1} will cause a {2} filter policy conflict for {3} from the following policies:

PAM-CMN-0886 = Adding {0} to group {1} will cause a {2} filter policy conflict for {3} from the following policies:

PAM-CMN-0887 = Policy settings for association will cause a {0} filter policy conflict for {1} and {2} from the following policies:

PAM-CMN-0888 = Not authorized to retrieve policy conflicts.

PAM-CMN-0889 = Policy conflicts exist in CA PAM. Navigate to the policy conflict page to view the conflicts.

PAM-CMN-0890 = Credential {0} from association between user {1} and device {2}.

PAM-CMN-0891 = Updating the group membership for {0} will cause a credential policy conflict for access method {1} on {2} from the following policies:

PAM-CMN-0892 = Adding {0} to group {1} will cause a credential policy conflict for access method {2} on {3} from the following policies:

PAM-CMN-0893 = Adding device {0} to {1} will cause a credential policy conflict for {2} for access method {3} from the following policies:

PAM-CMN-0894 = Adding access method {0} to {1} will cause a credential policy conflict for {2} from the following policies:

PAM-CMN-0895 = Adding {0} to group {1} will cause a credential policy conflict for {2} for access method {3} from the following policies:

PAM-CMN-0896 = Adding access method {0} to group {1} will cause a credential policy conflict for {2} on {3} from the following policies:

PAM-CMN-0897 = Policy settings for association will cause a credential policy conflict for {0} and access method {1} on {2} from the following policies:

PAM-CMN-0898 = Policy settings cause a credential conflict for secondary login. See your CA PAM Administrator and check the log for details.

## Authentication-Related Messages

PAM-CMN-0899 = Invalid authentication method: {0}.

PAM-CMN-0900 = Bad User ID ({0}) or Password.

PAM-CMN-0901 = You are not allowed to login at this time.

PAM-CMN-0902 = To login you have to accept the terms of the license.

PAM-CMN-0903 = This account is deactivated. See your CA PAM Administrator.

PAM-CMN-0904 = No Email Contact to Alert: {0}

PAM-CMN-0905 = Email alert sent to user {0}: {1}

PAM-CMN-0906 = User {0} deactivated due to reaching the password failure limit.

PAM-CMN-0907 = Account {0} has expired. See your CA PAM Administrator.

PAM-CMN-0908 = Account {0} is not yet activated. See your CA PAM Administrator.

PAM-CMN-0909 = Account {0} has been deactivated due to extended inactivity. See your CA PAM Administrator.

PAM-CMN-0910 = Unable to create security context for user {0}.

PAM-CMN-0911 = Due to account modifications, please change your password.

PAM-CMN-0912 = Due to password timeout, please change your password.

PAM-CMN-0913 = Due to increased password security, please change your password.

PAM-CMN-0914 = User {0} has logged into the CA Privileged Access Manager appliance {1}.

PAM-CMN-0915 = User {0} logged in.

PAM-CMN-0916 = This CA PAM appliance is in maintenance mode. Only admin level users can login.

PAM-CMN-0917 = User {0} logged in successfully via {1} authentication.

PAM-CMN-0918 = User deactivated.

PAM-CMN-0919 = Deactivated account {0}. Exceeded inactivity limit.

PAM-CMN-0920 = Deactivated account {0}. Account expired.

PAM-CMN-0921 = Single Sign On authentication failed. Please retry login.

PAM-CMN-0922 = You are logged out of CA PAM.

PAM-CMN-0923 = Single sign-on session expired. Please re-login.

PAM-CMN-0924 = Multiple CA PAM user accounts map to the same SAML identity ({0}). Rejecting the SAML authentication request and deactivating all the user accounts. Please activate one account that will be used to map to the SAML identity.

PAM-CMN-0925 = User {0} from SAML enabled group {1} has the same SAML user name {2} from SAML attribute {3}. User account deactivated.

PAM-CMN-0926 = Single sign-on authentication failed. Please contact your system administrator.

PAM-CMN-0927 = SAML user {0} not found in CA PAM or does not belong to a SAML enabled group.

PAM-CMN-0928 = SAML assertion {0} timestamp exceeds validity window by approximately {1} minutes. Assertion Issued: {2}.

PAM-CMN-0929 = SAML assertion issuer, {0}, does not match configured issuer {1}.

PAM-CMN-0930 = Invalid SAML assertion recipient URL: {0}.

PAM-CMN-0931 = SAML assertion recipient, {0}, not recognized. Valid recipients are: {1}.

PAM-CMN-0932 = SAML assertion received by authentication service at time {0} is before SAML Not-Before Condition {1}.

PAM-CMN-0933 = SAML assertion received by authentication service at time {0} is after SAML Not-On-Or-After Condition {1}.

PAM-CMN-0934 = SAML assertion received with a non-successful status code {0}.

PAM-CMN-0935 = CA PAM appliance in FIPS mode. SAML SSO disabled.

PAM-CMN-0936 = User attempted to login via SAML SSO but SAML SSO is not enabled.

PAM-CMN-0937 = SAML assertion not found in request.

PAM-CMN-0938 = Unable to decode SAML assertion.

PAM-CMN-0939 = SAML assertion failed schema validation.

PAM-CMN-0940 = Verification of SAML assertion failed: Certificate of SAML assertion producer has not been uploaded to CA PAM.

PAM-CMN-0941 = Saving the SAML assertion to a temporary file failed.

PAM-CMN-0942 = SAML assertion failed signature verification.

PAM-CMN-0943 = There are no user or user groups with an authentication method of SAML.

PAM-CMN-0944 = Login failed for user {0} due to multiple active RADIUS users having the same login name. All RADIUS users with login name {1} will be deactivated.

PAM-CMN-0945 = Login Failed. Please contact your system administrator for further assistance.

PAM-CMN-0946 = Authentication Daemon communication failure: {0}

PAM-CMN-0947 = Authentication Daemon access rejected message: {0}

PAM-CMN-0948 = Authentication Daemon General Error occurred ({0}). Please check if the Authentication Daemon is properly set up.

PAM-CMN-0949 = RADIUS user is not registered. Contact your CA PAM Administrator.

PAM-CMN-0950 = Authentication failed for RADIUS user {0}. RADIUS authentication succeeded but unable to retrieve the user's RADIUS group.

PAM-CMN-0951 = Authentication failed for RADIUS user {0}. RADIUS authentication succeeded but the user's RADIUS group changed from {1} to {2}. The new RADIUS group is not registered with CA PAM. User account deleted.

PAM-CMN-0952 = RADIUS user {0} moved from RADIUS group {1} to RADIUS group {2}.

PAM-CMN-0953 = Authentication failed for RADIUS user {0}. RADIUS authentication succeeded but the user's RADIUS group, {1}, is not registered. User will be logged out.

PAM-CMN-0954 = Adding RADIUS user {0} to CA PAM failed with message(s): {1}.

PAM-CMN-0955 = Authentication user {0} returned an invalid {1} challenge response for {2} authentication. Authentication request denied.

PAM-CMN-0956 = Unrecognized RADIUS challenge type {0}. Authentication request for user {1} denied.

PAM-CMN-0957 = SAML RADIUS authentication succeeded but the RADIUS group was not passed to CA PAM. User will be deleted and logged out.

PAM-CMN-0958 = Cisco SSO RADIUS user {0} moved to registered RADIUS group {1}.

PAM-CMN-0959 = User is not logged in.

PAM-CMN-0960 = Verify user credentials does not support the authentication method configured for the user.

PAM-CMN-0961 = User not found.

PAM-CMN-0962 = Determining the least-loaded CA PAM appliance for user ({0})'s session failed. Granting the user a session on this appliance.

PAM-CMN-0963 = Invalid attempt to acquire a session on this CA PAM appliance as user {0} via CA PAM load balance redirect.

PAM-CMN-0964 = Login failed for user {0} due to multiple active RSA users having the same login name. All RSA users with login name {1} will be deactivated.

PAM-CMN-0965 = Login Failed. Please contact your system administrator for further assistance.

PAM-CMN-0966 = User {0} selected to authenticate via {1} but the configured authentication method for the user is {2}.

PAM-CMN-0967 = The Active Directory user with user principal name {0} or samAccountName {1} is not registered with CA PAM.

PAM-CMN-0968 = The LDAP user with attribute {0}={1} is not registered with CA PAM

PAM-CMN-0969 = User {0} session is set for post-authentication load balancing to member {1}. The user's session will be destroyed on this member and resumed on member {2}.

PAM-CMN-0970 = User {0} session has been post-authentication load balanced to this member. The user's session will be resumed on this member.

PAM-CMN-0971 = User {0} failed LDAP+RSA authentication. The LDAP authentication failed.

PAM-CMN-0972 = User {0} failed LDAP+RSA authentication. The RSA authentication failed with RSA user name {1}.

PAM-CMN-0973 = User {0} attempted to access from an unauthorized IP: {1}. The only authorized networks are [{2}].

PAM-CMN-0974 = You have attempted to gain access from an invalid network. Please contact your administrator.

PAM-CMN-0975 = You have not been authorized to connect.

PAM-CMN-0976 = User {0} attempted an invalid PKI authentication.

PAM-CMN-0977 = PKI authentication failed with error: {0}

PAM-CMN-0978 = PKI user {0} not approved for access. Registration deleted.

PAM-CMN-0979 = LDAP authentication failed for user {0} with error code ({1}) and error string ({2}).

PAM-CMN-0980 = User {0} selected to authenticate via {1} but the user is required to authenticate via SAML from the SAML authentication inherited from the following group(s): {2}.

PAM-CMN-0981 = User {0} with authentication type SAML is mapped to the same SAML user name, {1}, as other CA PAM accounts. User account deactivated.

PAM-CMN-0982 = SAML SSO Authentication Failure: Status Code: {0}. Status Message: {1}. SubStatus Code: {2}.

PAM-CMN-0983 = Just-In-Time provisioning of user {0} failed because the userGroup attribute of the SAML assertion does not contain a valid CA PAM user group name. The groups specified in the SAML assertion are: {1}.

PAM-CMN-0984 = Just-In-Time provisioning of user {0} failed due to the following errors: {1}.

PAM-CMN-0985 = Just-In-Time provisioning of user {0} failed due to missing required attribute {1}.

PAM-CMN-0986 = SAML user {0} was not found on CA PAM but the remote identity provider {1} is configured for Just In Time provisioning. CA PAM will attempt to provision an account for the user in the following CA PAM groups: {2}.

PAM-CMN-0987 = The user initiated a SAML SSO Test to remote identity provider {0}.

PAM-CMN-0988 = The validation of the SAML assertion of user identity {0} from remote IdP {1} succeeded but mapping the user to a SAML-enabled CA PAM account failed.

PAM-CMN-0989 = User {0} logged in successfully via {1} authentication from remote IdP {2}.

PAM-CMN-0990 = A SAML reauthentication request was received for a password view request but the remote IdP entity ID is missing from the user's session.

PAM-CMN-0991 = The SAML reauthentication to view the password for account {0} failed: Status Code: {1}. Status Message: {2}. SubStatus Code: {3}.

PAM-CMN-0992 = The SAML reauthentication to view the password for account {0} failed: {1}.

PAM-CMN-0993 = The user attempted to verify their password to view an account password using SAML authentication but the user did not authenticate to CA PAM via SAML authentication.

PAM-CMN-0994 = The SAML reauthentication to view the password for account {0} failed. The user identity in the SAML assertion, {1}, does not match the identity of the CA PAM user that initiated the password view request.

PAM-CMN-0995 = Your LDAP password has been reset. You are required to change your password.

PAM-CMN-0996 = Your LDAP password has expired. You are required to change your password.

PAM-CMN-0997 = The user's LDAP domain is not configured with CA PAM to use TLS and therefore CA PAM will not enable the user to change their password.

PAM-CMN-0998 = User {0} logged in successfully via {1} authentication but will be required to change their password.

PAM-CMN-0999 = A user authenticated with login name {0} but a user with the specified login name is not registered with CA PAM.

PAM-CMN-1000 = User {0} failed LDAP+RADIUS authentication. The LDAP authentication failed.

PAM-CMN-1001 = User {0} failed LDAP+RADIUS authentication. The RADIUS authentication failed with RADIUS user name {1}.

PAM-CMN-1002 = PKI user(s) {0} not approved for access.

PAM-CMN-1003 = Invalid pending PKI user ids specified: {0}.

PAM-CMN-1004 = PKI user(s) {0} approved for access.

PAM-CMN-1005 = Unable to approve the pending PKI user {0} for access: {1}.

PAM-CMN-1006 = CA PAM as a SAML SP received an authentication request for unknown SAML identity provider {0}.

PAM-CMN-1007 = An error occurred while processing SAML assertion: {0}.

PAM-CMN-1008 = SAML SSO Authentication Failure: The received assertion did not include a subject name identifier nor the userName SAML attribute.

PAM-CMN-1009 = SAML password view request out-of-sync ({0} != {1}): The user's internal id did not match the id contained in the user's session.

PAM-CMN-1010 = Please accept the license to proceed.

PAM-CMN-1011 = The user was required to accept the license but canceled. Access denied.

PAM-CMN-1012 = The following group names contained in the SAML assertion do not exist in CA PAM and will be ignored in the Just In Time provisioning of the user {0}: {1}.

PAM-CMN-1013 = User {0} re-logged in successfully via {1} authentication.

PAM-CMN-1014 = User {0} failed {1} re-authentication.

PAM-CMN-1015 = Authentication type mismatch on re-authentication.

PAM-CMN-1016 = User mismatch on re-authentication.

PAM-CMN-1017 = Proxy authentication failed. Cannot find corresponding CA PAM user.

PAM-CMN-1018 = Configuration Password is still the default value.

PAM-CMN-1019 = PKI user {0} approved. User was created.

PAM-CMN-1020 = Attempt to approve PKI user {0} failed. Message was {1}.

PAM-CMN-1021 = SAML SSO of Just-In-Time provisioned user {0} failed due to missing required attribute {1}.

PAM-CMN-1022 = SAML SSO of Just-In-Time provisioned user {0} failed because the userGroup attribute of the SAML assertion does not contain a valid CA PAM user group name. The groups specified in the SAML assertion were: {1}.

PAM-CMN-1023 = The user groups of the Just-In-Time provisioned user {0} has been updated: {1}.

PAM-CMN-1024 = The user groups of the Just-In-Time provisioned user {0} has been updated: {1}. The following user groups contained in the assertion are not valid CA PAM user groups and will be ignored: {2}.

PAM-CMN-1025 = SAML SSO Authentication Failed: Updating the user groups of SAML SSO Just-In-Time provisioned user {0} failed: {1}



PAM-CMN-1026 = SAML SSO of Just-In-Time provisioned user {0} succeeded. The user's group membership has not changed. The assertion also contained the following group names that do not exist in CA PAM: {1}.

PAM-CMN-1027 = LDAP user account {0} is disabled in Active Directory.

PAM-CMN-3252 = Authentication failed. Please contact administrator or try again later.

PAM-CMN-3253 = User {0} failed to access device {1}. The primary site is unreachable and the cluster is configured for security-safe mode. Credentials cannot not be serviced from the local database in security safe mode.

PAM-CMN-3254 = Unauthorized access to RADIUS configuration.

PAM-CMN-3255 = Failed to save the RADIUS configuration on member {0}. Unable to establish a connection to the CA PAM appliance.

PAM-CMN-3256 = Saving RADIUS configuration on all cluster members failed for {0}/{1} members: {2}.

PAM-CMN-3257 = RADIUS configuration saved on all cluster members.

PAM-CMN-3258 = GateKeeper RADIUS configuration saved.

PAM-CMN-3259 = Failed to retrieve the RADIUS configuration from primary member {0}. Unable to establish a connection to the CA PAM appliance.

PAM-CMN-3260 = Synchronizing RADIUS configuration from primary cluster member {0} failed.

PAM-CMN-3261 = RADIUS configuration retrieved from primary cluster member successfully.

PAM-CMN-3263 = Gatekeeper RDPProxy configuration saved.

PAM-CMN-3264 = Failed to save the RDP configuration on member {0}. Unable to establish a connection to the CA PAM appliance.

PAM-CMN-3265 = Saving RDPProxy configuration on all cluster members failed for {0}/{1} members: {2}.

PAM-CMN-3266 = RDPProxy configuration saved on all cluster members.

PAM-CMN-3267 = Failed to retrieve the RDPProxy configuration from primary member {0}. Unable to establish a connection to the CA PAM appliance.

PAM-CMN-3268 = Synchronizing RDPProxy configuration from primary cluster member {0} failed.

PAM-CMN-3269 = RDPProxy configuration retrieved from primary cluster member successfully.

PAM-CMN-3351 = The Kerberos Authentication for the device "{0}" will be disabled because device is defined by IP address.

PAM-CMN-3352 = The Kerberos Authentication requires device to be defined by it's FQDN. Kerberos for the device "{0}" will be disabled.

PAM-CMN-3353 = The device "{0}" has more than one Kerberos KDC server defined for on Group level. Kerberos Authentication will be disabled until conflict is resolved.

## Access Service Messages

PAM-CMN-1029 = Task not enabled.

PAM-CMN-1030 = Unexpected command filter policy conflict - launch aborted.

PAM-CMN-1031 = Unexpected socket filter policy conflict - launch aborted.

PAM-CMN-1032 = Missing required device data - launch aborted.

PAM-CMN-1033 = Unauthorized attempt by user {0} to view the access page for user {1}.

PAM-CMN-1034 = Unexpected filter policy conflict - launch aborted.

PAM-CMN-1035 = Unexpected credential conflict - launch aborted.

PAM-CMN-1036 = Unauthorized attempt to set LDAP browser port.

PAM-CMN-1037 = Unauthorized attempt to update LDAP browser domain destination.

PAM-CMN-1038 = Unexpected AWS policy conflict - launch aborted.

PAM-CMN-1039 = AWS Policy {0} missing.

PAM-CMN-1040 = Unable to launch AWS Management Console. If this problem persists then ask your Administrator to investigate.

PAM-CMN-1041 = User {0} attempted to launch recorded web portal {1} but the mount is down. Due to the configured security safe policy, the user's connection attempt will be denied

PAM-CMN-1042 = User {0} attempted to launch recorded web portal {1} but the mount is down. Due to the configured operational safe policy, the user's connection attempt will be granted but not recorded.

PAM-CMN-1043 = CA PAM denied web portal {0}'s connection to host {1} because it does not match an entry in the web portal's access list.

PAM-CMN-1044 = CA PAM denied a request to proxy an HTTP connection to host {0} because the request could not be verified to have originated from an CA browser instance.

PAM-CMN-1045 = CA PAM denied the user's access to web portal {0}. The CA browser is not supported on the {1} operating system.

PAM-CMN-1046 = CA PAM denied user's unauthorized access to web portal {0} on host {1}.

PAM-CMN-1047 = CA PAM unable to find connection data authorizing service {0}'s access to host {1}.

PAM-CMN-1048 = CA PAM denied the user's access to web portal {0}. The CA browser requires a 32-bit JRE.

PAM-CMN-1049 = CA PAM denied the user's SSO access to the AWS Management Console with: invalid SSO credentials specified.

PAM-CMN-1050 = No Office365 HTML was generated.

PAM-CMN-1051 = Unable to launch Office 365 portal: Error code {0}: {1}.

PAM-CMN-1052 = Unable to launch Office 365 portal: Office 365 parameters are not configured.

PAM-CMN-1053 = Unable to launch Office 365 portal: Login credential not found.

PAM-CMN-1054 = Access to credential denied because authorization is required. Authorization request sent. Try again later.

PAM-CMN-1055 = Access to credential denied because the credential is already checked out by someone else. Try again later.

PAM-CMN-1056 = Access to credential denied because authorization request is still pending. Try again later.

PAM-CMN-1057 = Unable to generate AWS proxy account. Please contact CA PAM administrator

PAM-CMN-1058 = Unable to generate NSX proxy account. Please contact CA PAM administrator

PAM-CMN-1059 = The session URL does not match with the URL triggered by the UI

PAM-CMN-1060 = Access denied because of internal failure. Please contact CA PAM administrator.

PAM-CMN-1061 = Access denied because a credential was not chosen or is not available. Please launch the service and choose an available credential.

PAM-CMN-1062 = Access denied because dual authorization is required. If a password view request is not pending please launch the service to create one.

PAM-CMN-1063 = Proxy was not launched because the user failed to correctly respond to the pop up in time.

## Credential Management Messages

PAM-CMN-1064 = Credential daemon is not available.

PAM-CMN-1065 = Credential id not found.

PAM-CMN-1066 = No credential sources available.

PAM-CMN-1067 = Could not update or save credential. Check that the title is not already in use.

PAM-CMN-1068 = Password Authority invalid authentication.

PAM-CMN-1069 = Password Authority unavailable.

PAM-CMN-1070 = Unexpected error in source response.

PAM-CMN-1071 = This password is a privileged password; it cannot be used for single sign-on for target device.

PAM-CMN-1072 = No Password Authority username and password provided.

PAM-CMN-1073 = The credential service did not find a cryptographic encryption key. Regenerating key; existing credentials will be lost.

PAM-CMN-1074 = The credential service was not able to contact database.

PAM-CMN-1075 = The internal credential source storage is currently disabled by administrator.

PAM-CMN-1076 = The credential daemon has been given an invalid input.

PAM-CMN-1077 = The requested credential is corrupted or cannot be decrypted.

PAM-CMN-1078 = Unexpected error sent by credential daemon; please contact your administrator.

PAM-CMN-1079 = Credential not available. Please contact your administrator.

## View and Search Messages

PAM-CMN-1081 = Badly formed data - operation not performed

PAM-CMN-1082 = This view should be updated, not added.

PAM-CMN-1083 = View {0} not added.

PAM-CMN-1084 = Invalid search specified for view.

PAM-CMN-1085 = Duplicate view name.

## Cluster Management Messages

PAM-CMN-1086 = Unauthorized access to cluster configuration.

PAM-CMN-1087 = Passphrase is required to generate the shared cluster key.

PAM-CMN-1088 = Cluster shared key is required.

PAM-CMN-1089 = Cluster shared key must be a 40-character-long hexadecimal string.

PAM-CMN-1090 = The interface to use for cluster communications must be specified.

PAM-CMN-1091 = Invalid cluster interface specified. Valid values are {0}.

PAM-CMN-1092 = Virtual Management IP Address is required.

PAM-CMN-1093 = Virtual Management IP Address must be a valid IP address.

PAM-CMN-1094 = Virtual Management IP Domain Name must be a valid hostname.

PAM-CMN-1095 = Invalid cluster member list specified.

PAM-CMN-1096 = Cluster must contain at least two members, including this CA PAM appliance.

PAM-CMN-1097 = The IP address specified for this CA PAM appliance in the cluster member list cannot be assigned to the cluster interface.

PAM-CMN-1098 = This CA PAM appliance must be a member of the cluster.

PAM-CMN-1099 = The subnet of the CA PAM appliance cluster interface is required.

PAM-CMN-1100 = Invalid cluster subnet format specified.

PAM-CMN-1101 = Invalid cluster subnet network address {0}.

PAM-CMN-1102 = Invalid cluster subnet network mask {0}.

PAM-CMN-1103 = The specified cluster subnet does not have enough host addresses ({0}) for all cluster members ({1}).

PAM-CMN-1104 = The specified NAT address {0} is not a valid IP address or hostname.

PAM-CMN-1105 = The specified PAT address {0} is not a valid IP address or hostname.

PAM-CMN-1106 = The specified PAT port {0} is not a valid port number.

PAM-CMN-1107 = Failed to authenticate to cluster member {0}. Please confirm that the shared key has been configured on the cluster member.

PAM-CMN-1108 = Failed to save the cluster configuration on member {0}. Error(s) received: {1}

PAM-CMN-1109 = Failed to save the cluster configuration on member {0}. Unable to establish a connection to the CA PAM appliance.

PAM-CMN-1110 = Failed to start the cluster due to configuration errors.

PAM-CMN-1111 = The cluster configuration values do not match for fields: {0}.

PAM-CMN-1112 = Failed to start the cluster. The cluster configuration on members {0} and {1} are not the same. The errors reported by {2} are: {3}.

PAM-CMN-1113 = Failed to start the cluster. Unable to check for consistent cluster configuration on member {0}. The remote errors reported are: {1}.

PAM-CMN-1114 = Failed to start the cluster. Unable to establish a connection to member {0}.

PAM-CMN-1115 = Failed to start the cluster. Configuring the replication interface on member {0} failed.

PAM-CMN-1116 = Failed to start the cluster. Unable to successfully ping cluster member {0}.

PAM-CMN-1117 = Failed to start the cluster. Unable to retrieve hostname data from cluster member {0}.

PAM-CMN-1118 = Failed to start the cluster. Unable to save hostname data on cluster member {0}.

PAM-CMN-1119 = Failed to stop the cluster on member {0}: {1}

PAM-CMN-1120 = Failed to stop the cluster due to configuration errors.



PAM-CMN-1121 = Failed to start the cluster. Unable to configure and start the cluster runtime.  
PAM-CMN-1122 = Failed to configure the cluster runtime on member {0}.  
PAM-CMN-1123 = Starting the cluster runtime has failed.  
PAM-CMN-1124 = Starting the cluster runtime on member {0} has failed.  
PAM-CMN-1125 = Unable to start cluster members {0}.  
PAM-CMN-1126 = The specified CA PAM appliance is not a member of the cluster.  
PAM-CMN-1127 = Failed to stop cluster member {0} due to configuration errors.  
PAM-CMN-1128 = Failed to start cluster member {0}: {1}  
PAM-CMN-1129 = The cluster interface, {0}, is already in use on cluster member {1}.  
PAM-CMN-1130 = Unable to make a connection to the remote CA PAM appliance {0}.  
PAM-CMN-1131 = The cluster must be enabled before starting or stopping individual cluster members.  
PAM-CMN-1132 = Starting the cluster ...  
PAM-CMN-1133 = Checking the consistency of the cluster configuration across all members ...  
PAM-CMN-1134 = Starting the cluster failed. Checking the cluster configuration consistency failed for {0} member(s): {1}.  
PAM-CMN-1135 = Computing the addresses to assign to the cluster interfaces ...  
PAM-CMN-1136 = Assigning computed addresses to the cluster interfaces ...  
PAM-CMN-1137 = Assigning computed addresses to the cluster interface failed for member(s): {0}.  
PAM-CMN-1138 = Verifying that all cluster interfaces have been properly configured ...  
PAM-CMN-1139 = Pinging all cluster members using the configured cluster interface failed for member(s): {0}.  
PAM-CMN-1140 = Assigning internal hostnames to cluster members ...  
PAM-CMN-1141 = Assigning internal hostnames to cluster members failed for member(s): {0}.  
PAM-CMN-1142 = Configuring the cluster runtime ...  
PAM-CMN-1143 = Starting the cluster runtime ...  
PAM-CMN-1144 = The cluster is online.  
PAM-CMN-1145 = Starting the cluster master on member {0} ...  
PAM-CMN-1146 = Attempt {0}/{1}: Checking if the master is online ...  
PAM-CMN-1147 = The cluster master is online. Starting the remaining cluster member(s) ...  
PAM-CMN-1148 = Starting the cluster has failed. Unable to start the cluster master {0}.  
PAM-CMN-1149 = Attempt {0}/{1}: Waiting for {2}/{3} member(s) to come online ...  
PAM-CMN-1150 = Cluster member {0} is now online.  
PAM-CMN-1151 = Cluster member {0} failed.  
PAM-CMN-1152 = Starting the cluster has failed: Unable to start cluster member(s): {0}.  
PAM-CMN-1153 = Stopping the cluster ...  
PAM-CMN-1154 = Stopping the cluster on member {0}...  
PAM-CMN-1155 = Cluster member {0} stopped.  
PAM-CMN-1156 = Stopping the cluster failed on {0}/{1} member(s): {2}.  
PAM-CMN-1157 = Cluster successfully stopped.  
PAM-CMN-1158 = Starting cluster member {0} ...  
PAM-CMN-1159 = Cluster started on member {0}.  
PAM-CMN-1160 = Attempt {0}/{1}: Waiting for member to come online ...  
  
PAM-CMN-1162 = This cluster node received a remote API call from source {0} with an incorrect shared key: {1}.  
PAM-CMN-1163 = Unauthorized attempt to retrieve cluster logs on this node. The shared key did not match.  
  
PAM-CMN-1460 = Saved cluster config locally. Virtual IP: {0}. Virtual IP FQDN: {1}. Cluster members: {2}. Status: OFF.  
PAM-CMN-1461 = ERROR: NTP problem on member {0}. {1}  
PAM-CMN-1462 = ERROR: Release level of member {0} ({1}) does not match primary member ({2})  
PAM-CMN-1463 = Saved cluster config to all cluster members. Cluster members: {0}. Status: {1}.  
PAM-CMN-1464 = External synchronization unlocked while in cluster-stopped mode  
PAM-CMN-1465 = External synchronization locked while in cluster-stopped mode  
PAM-CMN-1466 = Turned cluster on  
PAM-CMN-1467 = SEVERE: Unable to turn on the cluster because one or more cluster members failed cluster start checks.

PAM-CMN-1673 = User {0} using API key {1} can't perform {2} operations while cluster is stopped. {3} was not executed.

PAM-CMN-1675 = User {0} using API key {1} can't perform {2} operations while cluster is stopped. {3} was not executed.

PAM-CMN-1760 = Unauthorized attempt to check synchronization status of the cluster by {0}

PAM-CMN-1761 = Cluster started.

PAM-CMN-1762 = Cluster member {0} restarted.

PAM-CMN-1763 = Cluster configuration deleted.

PAM-CMN-1881 = Cannot delete - used for PAM Cluster Synchronization. Change the provision row used on the PAM Cluster Synchronization page before deleting.

PAM-CMN-1888 = GateKeeper cluster configuration from cluster member {0} saved. Cluster Shared Key: {0}. Cluster Replication Interface: {1}. Cluster Members: {2}. Cluster VIP Address: {3}. Cluster VIP FQDN: {4}. Cluster Subnet: {5}. Cluster Status: {6}.

PAM-CMN-1889 = GateKeeper cluster configuration saved. Cluster Shared Key: {0}. Cluster Replication Interface: {1}. Cluster Members: {2}. Cluster VIP Address: {3}. Cluster VIP FQDN: {4}. Cluster Subnet: {5}. Cluster Status: {6}.

PAM-CMN-1891 = Saving cluster configuration on all cluster members failed for {0}/{1} member(s): {2}.

PAM-CMN-1892 = Cluster configuration saved on all cluster members.

PAM-CMN-1959 = As the primary member, starting the polling of all cluster members until the database is synced across the cluster ...

PAM-CMN-1960 = Polling database sync status for member {0} (ELAPSED TIME = {1}) ...

PAM-CMN-1961 = Database sync on member {0} completed. (ELAPSED TIME = {1})

PAM-CMN-1962 = Database is still syncing on member {0} (ELAPSED TIME = {1}) ...

PAM-CMN-1963 = All databases done syncing, starting the Password Authority subsystem on each member in sequence (ELAPSED TIME = {0})

PAM-CMN-1966 = Password Authority subsystem started on all cluster members

PAM-CMN-1967 = SEVERE: License check failed. Stopping clustering on this node!

PAM-CMN-1968 = Requesting a full database from the primary member ...

PAM-CMN-1969 = Database dump is ready on the primary member. Retrieving the dump ...

PAM-CMN-1970 = Downloading the database dump from the primary member ...

PAM-CMN-1971 = CRC verification on the primary database OK. Downloading database cluster TLS certificates ...

PAM-CMN-1972 = Dump integrity check failed: Dump completed marker not found!

PAM-CMN-1973 = Dump integrity check failed: The number of tables in the dump ({0} != {1}) are incorrect!

PAM-CMN-1974 = All integrity checks passed, proceeding to loading master database ...

PAM-CMN-1975 = SEVERE: CRC verification on the primary database dump FAILED. Please stop the cluster and retry

PAM-CMN-1976 = SEVERE: Integrity checks on the database dump failed. Retrying downloading the database data ({0}) ...

PAM-CMN-1977 = Loading the database from the primary member completed successfully.

PAM-CMN-1978 = Sync with the primary member completed.

PAM-CMN-2353 = Turned cluster off

PAM-CMN-2551 = SEVERE: Repeated attempts to assign the VIP to this cluster member has failed! No more attempts to assign the VIP to this member will be made until the next cluster restart.

PAM-CMN-2552 = Making attempt {0} to assign the VIP to this cluster member ...

PAM-CMN-2553 = The VIP has been successfully assigned to this cluster member after %d attempts.

PAM-CMN-2554 = WARNING: VIP Assignment Failed! The Password Authority subsystem is down (it may be in the process of starting up)

PAM-CMN-2555 = SEVERE: Assigning the VIP to this cluster member failed.

PAM-CMN-2556 = SEVERE: VIP assignment failure limit reached! No further attempts will be made to assign the VIP to this cluster member until the next cluster restart!

PAM-CMN-2557 = SEVERE: Member {0} has failed to respond to heartbeat messages for 20 seconds; connection marked as down. The gateway is currently {1}

PAM-CMN-2558 = Initial connection for heartbeat messages to member {0} has been established. The gateway is currently {1}.

PAM-CMN-2559 = WARNING: Member {0} has resumed responding to heartbeat messages after an outage lasting {1} min(s) and {2} second(s). The gateway is currently {3}.

PAM-CMN-2560 = SEVERE: Connectivity to all members in the cluster has been lost but the gateway is reachable, maintaining Password Authority services and assuming the VIP address.

PAM-CMN-2561 = SEVERE: Connectivity to all members in the cluster has been lost and the gateway is unreachable, shutting down Password Authority services on this member to maintain data integrity.

PAM-CMN-2562 = WARNING: At least one other member in the cluster is now reachable, rejoining the cluster ...

PAM-CMN-2563 = Retrieving the primary database from cluster member {0} to resync my database.

PAM-CMN-2564 = SEVERE: Syncing with the primary database failed!

PAM-CMN-2565 = Resyncing with the primary database completed!

PAM-CMN-2566 = I am the only member alive and making attempt #{0} to assume the VIP.

PAM-CMN-2567 = WARNING: I should own the VIP but I do not. Assuming the VIP ...

PAM-CMN-2568 = Cluster starting ...

PAM-CMN-2569 = Retrieving primary database from cluster member {0} ...

PAM-CMN-2570 = Syncing the database with the primary cluster member succeeded.

PAM-CMN-2571 = SEVERE: Syncing the database with the primary cluster member failed!

PAM-CMN-2572 = I am the primary member in the cluster. All cluster members will sync with my database.

PAM-CMN-2573 = WARNING: I currently own the VIP but there is a cluster member that is alive with a higher precedence. Releasing the VIP.

PAM-CMN-2574 = Can't remove current server.

PAM-CMN-2575 = Failed to update current server: server was removed but new server was not added. Please check if connection was established.

PAM-CMN-2576 = Can't update current server: failed to remove server. Please check if connection was established.

PAM-CMN-2596 = The device lost Ethernet link while in clustering mode. Locking.

PAM-CMN-2622 = SEVERE: Download of the primary database dump FAILED. Please stop the cluster and retry

PAM-CMN-2623 = Downloading the database dump CRC from the primary member ...

PAM-CMN-2624 = Database dump and CRC downloaded. Verifying CRC ...

PAM-CMN-2625 = SEVERE: Download of the database cluster TLS certificates FAILED. Please stop the cluster and retry

PAM-CMN-2626 = Downloading the database cluster TLS certificates CRC from the primary member ...

PAM-CMN-2627 = SEVERE: Download of the primary database dump CRC FAILED. Please stop the cluster and retry

PAM-CMN-2628 = SEVERE: Download of the database cluster TLS certificates CRC FAILED. Please stop the cluster and retry

PAM-CMN-2629 = SEVERE: CRC verification on the primary database TLS certificates FAILED. Please stop the cluster and retry

PAM-CMN-2630 = CRC verification on the primary database TLS certificates OK. Downloading NIM SM database and properties...

PAM-CMN-2631 = SEVERE: Download of the NIM SM properties FAILED. Please stop the cluster and retry

PAM-CMN-2632 = SEVERE: Download of the NIM SM database FAILED. Please stop the cluster and retry

PAM-CMN-2633 = Downloading the NIM SM CRC from the primary member...

PAM-CMN-2634 = SEVERE: Download of the NIM SM CRC FAILED. Please stop the cluster and retry

PAM-CMN-2635 = SEVERE: CRC verification on the primary NIM SM FAILED. Please stop the cluster and retry

PAM-CMN-2743 = Cluster member {0} of site {1} has left the cluster.

PAM-CMN-2744 = Node {0} was added to site {1} of an active cluster.

PAM-CMN-2745 = This configuration will be replicated to all cluster members

PAM-CMN-2746 = The delete action will be performed on all cluster members

PAM-CMN-2752 = The database of this node, {0}, is out of sync with the primary database. The cluster or node should be resynced as soon as possible to resynchronize this node with the cluster.

PAM-CMN-2756 = The secondary site member {0} is now active.

PAM-CMN-2757 = The secondary site member {0} is inactive and will remain inactive until replication catches up to the primary site or the member is manually resynced.

PAM-CMN-2758 = This secondary site member {0} has lost connection to the primary site for {1} since {2}.

PAM-CMN-2759 = The primary site has lost contact with secondary site member {0} for {1} since {2}.

PAM-CMN-2760 = This secondary site member, {0}, is inactive since {1} and will remain active until resynced with the primary site.

PAM-CMN-2763 = A lag in replication has been detected between the database of this member and the primary database.

PAM-CMN-2764 = The connection timed-out checking whether this member's database is consistent with the primary database.

PAM-CMN-2765 = The database of this member is out-of-sync with the primary database.

PAM-CMN-2766 = The database of this member is in-sync with the primary database.

PAM-CMN-2769 = The credential management subsystem of this secondary member has failed to contact the primary site.

PAM-CMN-2770 = The credential management subsystem of this secondary member has lost contact with the primary site for longer than {0} seconds.

PAM-CMN-2771 = The credential management subsystem of this secondary member has lost contact with the primary site for longer than {0} seconds.

PAM-CMN-2772 = The credential management subsystem of this secondary member is connected to the primary site.

PAM-CMN-2773 = Primary site members are always active.

PAM-CMN-2774 = This secondary site member is active.

PAM-CMN-2775 = This secondary site member has been deactivated for lagging in replication for more than {0} minutes behind the primary site.

PAM-CMN-2776 = The Credential Management services of this node are locked due to the state of the cluster. No credentials can be viewed or used in autoconnect.

PAM-CMN-2777 = The request from user {0} to view credential {1} was denied due to the primary site being unreachable and this node being configured in security safe mode.

PAM-CMN-2778 = Starting Credential Management on this member ...

PAM-CMN-2779 = Password Authority subsystem started successfully on this node (ELAPSED TIME = {0})

PAM-CMN-2780 = Requesting the primary site to activate my site, {0} ...

PAM-CMN-2781 = Password Authority subsystem startup initiated on node {0} (ELAPSED TIME = {1})

PAM-CMN-2782 = Waiting for all Password Authority subsystems to complete startup ... (ELAPSED TIME = {0})

PAM-CMN-2783 = Only queries against configuration table are allowed with ConfigService->dbQuery()

PAM-CMN-2784 = Device Console fields are deprecated.

PAM-CMN-2785 = Power device is deprecated.

PAM-CMN-2786 = Special Type Device is deprecated.

PAM-CMN-2787 = The connection timed-out checking whether the member {0}'s database is consistent with the primary database for {1} seconds since {2}.

PAM-CMN-2788 = The database of the member {0} is out-of-sync with the primary database for {1} seconds since {2}.

PAM-CMN-2789 = The database of the member {0} is in-sync with the primary database now.

PAM-CMN-2792 = A CSV import job has completed on this node and the updates are being replicated across the cluster. Please wait until it is complete before initiating another.

PAM-CMN-2793 = A CSV import job has completed on this node and the updates are being replicated across the cluster. Elapsed time is {0}.

PAM-CMN-2794 = The database status of this member is not known. This commonly happens when a new member is subscribing to the cluster. Please press the Refresh Replication Status button for the current status.

PAM-CMN-2874 = This primary clustered PAM does not have commit permission to the RFS. You must run 'rfs-setup --gang-client' on the RFS first.

PAM-CMN-2931 = WARNING: I currently own the VIP but there is a cluster member that is alive with a higher precedence. Releasing the VIP.

PAM-CMN-2933 = Making attempt {0} to assign the VIP to this cluster member...

PAM-CMN-2936 = SEVERE: Repeated attempts to assign the VIP to this cluster member has failed! No more attempts to assign the VIP to this member will be made until the next cluster restart.

PAM-CMN-2937 = The VIP has been successfully assigned to this cluster member after {0} attempts.

PAM-CMN-2938 = WARNING: VIP Assignment Failed! The Password Authority subsystem is down (it may be in the process of starting up)

PAM-CMN-2939 = SEVERE: Assigning the VIP to this cluster member failed.

PAM-CMN-2940 = SEVERE: VIP assignment failure limit reached! No further attempts will be made to assign the VIP to this cluster member until the next cluster restart!

PAM-CMN-2941 = SEVERE: Member {0} has failed to respond to heartbeat messages for 20 seconds; connection marked as down. The gateway is currently {1}.

PAM-CMN-2942 = Initial connection for heartbeat messages to member {0} has been established. The gateway is currently {1}.

PAM-CMN-2943 = WARNING: Member {0} has resumed responding to heartbeat messages after an outage lasting {1} min(s) and {2} second(s). The gateway is currently {3}.

PAM-CMN-2944 = SEVERE: Connectivity to all members in the cluster has been lost but the gateway is reachable, maintaining Password Authority services and assuming the VIP address.

PAM-CMN-2945 = SEVERE: Connectivity to all members in the cluster has been lost and the gateway is unreachable, shutting down Password Authority services on this member to maintain data integrity.

PAM-CMN-2947 = WARNING: At least one other member in the cluster is now reachable, rejoining the cluster...

PAM-CMN-2948 = Retrieving the primary database from cluster member {0} to resync my database

PAM-CMN-2949 = SEVERE: Syncing with the primary database failed!

PAM-CMN-2950 = Resyncing with the primary database completed!

PAM-CMN-2952 = I am the only member alive and making attempt #{0} to assume the VIP.

PAM-CMN-2953 = WARNING: I should own the VIP but I do not. Assuming the VIP...

PAM-CMN-2954 = Cluster starting...

PAM-CMN-2955 = \* Restarted to recognize site membership update

PAM-CMN-2957 = Syncing the database with the primary cluster member succeeded.

PAM-CMN-2958 = SEVERE: Starting up Credential Management on this node failed!

PAM-CMN-2959 = SEVERE: Starting up Credential Management on all nodes in secondary site failed!

PAM-CMN-2960 = SEVERE: Syncing the database with the primary cluster member failed

PAM-CMN-2961 = All other nodes were unavailable to donate their database, therefore skipping DB sync and restarting PA on my own

PAM-CMN-2962 = I am the primary member in the cluster. All cluster members will sync with my database.

PAM-CMN-2963 = SEVERE: Starting up Credential Management on all nodes failed!



PAM-CMN-2964 = I am a node in a secondary site, will retrieve master database from the secondary site leader {0}  
PAM-CMN-2965 = I am a node in a secondary site, but its secondary leader is not available, will retrieve master database from {0} at the primary site  
PAM-CMN-2966 = I am a leader node in a secondary site, will retrieve master database from {0} at the primary site  
PAM-CMN-2967 = Start daily DB backup for cluster replication  
PAM-CMN-2976 = Backup DB failed!  
PAM-CMN-2977 = Backup DB succeed!  
PAM-CMN-2978 = Start to purge DB binary logs with the last {0} days logs  
PAM-CMN-2979 = Purge DB binary log failed!  
PAM-CMN-2980 = Purge DB binary log succeed!  
PAM-CMN-2981 = Skip daily DB backup because cluster is not turned on  
PAM-CMN-3143 = Releasing the VIP  
PAM-CMN-3144 = Assuming the VIP  
PAM-CMN-3145 = Communication Link Down  
PAM-CMN-3146 = Cannot communicate with other cluster members, but the Gateway is UP, Promoting to VIP  
PAM-CMN-3147 = Cannot communicate with other cluster members, disabling credential management services on this node and disabling cluster orchestration daemon  
PAM-CMN-3148 = This node will pull the database from the primary node  
PAM-CMN-3149 = Syncing this node's database with the primary database...  
PAM-CMN-3150 = Starting up Credential Management on this node failed!  
PAM-CMN-3151 = Starting up Credential Management on all nodes in secondary site failed  
PAM-CMN-3152 = Syncing the database with the primary cluster member failed!  
PAM-CMN-3153 = Starting up Credential Management on all nodes failed  
PAM-CMN-3226 = Cluster orchestration updating configuration to reflect site membership update

## Multi-Site Clustering Messages

PAM-CMN-2853 = This clustered member is not a member of the primary site. Please perform this operation on the primary member in the primary site!  
PAM-CMN-2854 = This clustered member is not the primary. Please perform this operation on the primary member!  
PAM-CMN-2855 = This cluster is currently ON. Please stop the cluster before performing this operation!  
PAM-CMN-2856 = Not all members of the cluster are reachable.  
PAM-CMN-2857 = The passphrase must be at least 16 characters long and contain one of [0-9][a-z][A-Z].  
PAM-CMN-2858 = Failed to securely cache the password.  
PAM-CMN-2859 = The encryption test of FIPS mode cryptography provider failed!  
PAM-CMN-2860 = Unknown cryptography provider!  
PAM-CMN-2861 = PAM will now reboot for this change to take effect.  
PAM-CMN-5057 = The maximum replication lag before secondary member deactivation must be specified  
PAM-CMN-5058 = Successfully saved cluster configuration to all members.  
PAM-CMN-5060 = The entered shared keys do not match!  
PAM-CMN-5061 = Site name not specified for site #{0}  
PAM-CMN-5062 = Site name for site #{0} is not valid: valid characters are alphanumeric, space, underscore and hyphen.  
PAM-CMN-5063 = Duplicate site name {0}  
PAM-CMN-5064 = Cluster must contain at least two members, including this member.  
PAM-CMN-5065 = The primary site must be specified

PAM-CMN-5066 = Invalid primary site index specified, valid values are 0-{0}

PAM-CMN-5067 = Invalid value specified for the maximum number of queued events before a site is deactivated. Valid values are between 500 and 100000 events

PAM-CMN-5069 = The cluster database consistency check period must be specified

PAM-CMN-5070 = Invalid value specified for the cluster database consistency check period. Valid values are between 5 and 1440 minutes

PAM-CMN-5075 = Multi-site operationally or security safe mode must be selected

PAM-CMN-5076 = Invalid value specified for the multi-site operationally or security safe mode. Valid values are operational and security

PAM-CMN-5077 = Invalid Database Replication Connection Timeout specified {0}. Valid values are between 5 and 90 seconds

PAM-CMN-5078 = Invalid Database Replication Socket Timeout specified {0}. Valid values are between 5 and 90 seconds

PAM-CMN-5079 = Duplicate address in cluster member list {0}: {1}

PAM-CMN-5080 = Invalid IP address or host name {0}: {1}

PAM-CMN-5081 = Changes have not been saved. This CA PAM member is not part of the member list. Please add your member IP to one of the existing sites below.

PAM-CMN-5082 = Failed to uniquely identify the site of this CA PAM member in the cluster configuration.

PAM-CMN-5083 = Unable to turn on the cluster because one or more cluster members failed cluster start checks. {0}

PAM-CMN-5084 = Turning the cluster on failed{0}

PAM-CMN-5085 = Cluster turned on successfully.

PAM-CMN-5086 = Cluster turned off successfully.

PAM-CMN-5087 = This node is unlocked. Scheduled jobs and processes that may trigger credential rotation will be allowed on this node. {0}

PAM-CMN-5088 = This node must remain the first member in the primary site when the cluster is restarted or all changes will be lost after cluster restart.

PAM-CMN-5089 = This node must be promoted to be the first member in the primary site when the cluster is restarted or all changes will be lost after cluster restart.

PAM-CMN-5090 = Site {0} must be promoted to be the primary site and this member must be promoted to be the first member in the site when the cluster is restarted or all changes will be lost after cluster restart.

PAM-CMN-5091 = This node must remain the first member in the cluster list when the cluster is restarted or all changes will be lost after cluster restart.

PAM-CMN-5092 = This node must be promoted to be the first member in the cluster list when the cluster is restarted or all changes will be lost after cluster restart.

PAM-CMN-5093 = Resyncing of {0} has failed. {1}

PAM-CMN-5094 = Resyncing of {0} has succeeded

PAM-CMN-5095 = Resyncing node {0} from site {1} with primary site

PAM-CMN-5096 = Resyncing site {0}.

PAM-CMN-5097 = Resyncing the selected site failed. {0}

PAM-CMN-5098 = The donor member is {0}.

PAM-CMN-5099 = Unable to find a member with an active database from the primary site

PAM-CMN-5100 = Resync site failed, the following members of the site are unresponsive: {0}

PAM-CMN-5101 = Resyncing the selected site succeeded.

PAM-CMN-5102 = The specified member is not part of a multisite enabled cluster{0}

PAM-CMN-5103 = CAN NOT CONNECT TO MEMBER: {0}

PAM-CMN-5104 = Member is successfully removed from the cluster.

PAM-CMN-5105 = This member cannot leave the cluster. The site must have at least one remaining member

PAM-CMN-5106 = Failed to update member {0}, it isn't alive

PAM-CMN-5107 = Stopping the cluster ...

PAM-CMN-5108 = Member successfully joined the cluster.

PAM-CMN-5109 = The number of sites cannot be modified as part of joining an active cluster.

PAM-CMN-5110 = Adding a new member to the primary site requires a cluster restart.

PAM-CMN-5111 = This node can only be added as a member of a secondary site. No other changes to the site member list are allowed.

PAM-CMN-5112 = CURL request to {0} returned error ({1}): {2}

PAM-CMN-5113 = NTP on this member is not properly configured

PAM-CMN-5114 = The release level of the cluster ({0}), does not match the release level of this node ({1})

PAM-CMN-5115 = The locale of the cluster ({0}), does not match the locale of this node ({1})

PAM-CMN-5116 = The license of this node does not match the license of the cluster: {0}

PAM-CMN-5117 = All members for site count {0} are

PAM-CMN-5118 = Member: {0}=> Cannot Communicate with Member. Please make sure the member is reachable and required ports are open.

PAM-CMN-5119 = Member: {0}=> License Mismatch ({1}). Please check your configuration and try again.

PAM-CMN-5120 = Member: {0}=> Access Denied. Please check your configuration and try again.

PAM-CMN-5121 = Member: {0}=> Inconsistent Member List (Click Save To Cluster).

PAM-CMN-5122 = Member: {0}=> OK.

PAM-CMN-5123 = The cluster was in a bad state.

PAM-CMN-5124 = The Credential Manager databases were still active on nodes:

PAM-CMN-5125 = The Session Manager databases were out of sync. Send system logs to CA for more information.

PAM-CMN-5126 = The administrator who performed this action was given guidance regarding how to remedy this, and those recommendations were acknowledged before the cluster was stopped.

PAM-CMN-5127 = Cluster-off operation initiated

PAM-CMN-5128 = {0}: NTP not properly configured.

PAM-CMN-5129 = {0}: release level, {1}, does not match primary release level ({2}).

PAM-CMN-5130 = ERROR: Locale of member {0} ({1}) does not match primary member ({2})

PAM-CMN-5131 = {0}: locale does not match primary.

PAM-CMN-5132 = Primary Site cannot be deleted.

PAM-CMN-5133 = Couldn't save the config file: {0}.

PAM-CMN-5134 = Site deleted.

PAM-CMN-5135 = {0} SAVING FAILED - {1}.

PAM-CMN-5136 = {0} STATUS OK.

PAM-CMN-5137 = Sending Cluster Stopped Failed On Some Members: {0}

PAM-CMN-5138 = all are for sendClusterStopped command: {0}

PAM-CMN-5139 = all are for saveRemote command: {0}

PAM-CMN-5140 = An error occurred while saving AWS provision.

PAM-CMN-5141 = Configuration successfully saved

PAM-CMN-5142 = Save to cluster failed for following reasons: {0}

PAM-CMN-5143 = This CA PAM node is part of the cluster and it is in the process of syncing. Try again later. Click <a href="/logoff.php">here</a> to login.

PAM-CMN-5144 = CA PAM server is starting up. Please try again later. Click <a href="/logoff.php">here</a> to login.

PAM-CMN-5145 = ERROR: Cluster member {0} is unable to connect to the primary using address {1}.

PAM-CMN-5146 = Cluster member {0} is unable to connect to the primary using address {1}.

PAM-CMN-5147 = Reboot is needed to enable LUNA-PCI changes

PAM-CMN-5148 = The FIPS mode of the cluster ({0}), does not match the FIPS mode of this node ({1})

PAM-CMN-5149 = ERROR: FIPS mode of member {0} ({1}) does not match primary member ({2})

PAM-CMN-5150 = {0}: FIPS mode does not match primary.

PAM-CMN-5151 = SEVERE: Requesting a full database from the primary member timed-out.

PAM-CMN-5152 = As the primary member, checking the polling status of member timed-out...

PAM-CMN-5153 = Could not change the login name of the administrator

PAM-CMN-5154 = User did not enter correct password for administrator login

PAM-CMN-5155 = The cryptographic provider of this node must be {0} to match the cryptographic provider of cluster



PAM-CMN-5156 = ERROR: The cryptographic provider of this node {0} must be {1} to match the cryptographic provider of primary node

PAM-CMN-5157 = {0}: The cryptographic provider must be {1} to match primary.

PAM-CMN-5158 = The cluster is not currently turned on.

PAM-CMN-5159 = The hardware platform of the cluster ({0}), does not match the hardware platform of this node ({1})

PAM-CMN-5160 = ERROR: hardware platform of member {0} ({1}) does not match the site leader member {2} ({3})

PAM-CMN-5161 = {0}: hardware platform does not match the site leader member {1}.

PAM-CMN-5162 = ERROR: The site hardware platform is {0} ({1}), but a provision key {2} is provided.

PAM-CMN-5163 = {0} ({1}): hardware platform does not match the provision key {2}.

PAM-CMN-5164 = ERROR: The site hardware platform is {0} ({1}), but no provision key {2} is provided.

PAM-CMN-5165 = {0}: The provision key {1} is missing for the hardware platform {2}.

PAM-CMN-5166 = Invalid provision key specified {0}. Can't have both AWS provision key and Azure provision key at the same time.

PAM-CMN-5167 = Adding a new site to the active cluster

PAM-CMN-5168 = The site {0} has been removed from the cluster

PAM-CMN-5169 = At least two sites are required for multi-site cluster. No site is allowed to be removed from the cluster

PAM-CMN-5170 = Invalid site index

PAM-CMN-5171 = Only one new site can be added at one time when the cluster is active

PAM-CMN-5172 = The number of site names doesn't match the site count

PAM-CMN-5173 = Removing the site {0} from the cluster

PAM-CMN-5174 = The site {0} has been successfully removed from the cluster

PAM-CMN-5175 = The total members in the primary site can not be more than 9

PAM-CMN-5176 = The total members of the cluster can not be more than 1000

PAM-CMN-5177 = The maximum replication lag before secondary member warning must be specified

PAM-CMN-5178 = The maximum replication lag before secondary member out-of-sync must be specified

PAM-CMN-5179 = Invalid value specified for the max replication before secondary member warning

PAM-CMN-5180 = Invalid value specified for the max replication lag before secondary member out of sync. Must be larger than warning value.

PAM-CMN-5181 = Invalid value specified for the max replication lag before secondary member deactivation. Must be larger than out-of-sync value.

PAM-CMN-5182 = The hardware platform of the cluster ({0}), does not match the hardware platform of this node ({1})

PAM-CMN-5183 = ERROR: hardware platform of member {0} ({1}) does not match the site leader member {2} ({3})

PAM-CMN-5184 = {0}: hardware platform does not match the site leader member {1}.

PAM-CMN-5185 = ERROR: The site hardware platform is {0} ({1}), but a provision key {2} is provided.

PAM-CMN-5186 = {0} ({1}): hardware platform does not match the provision key {2}.

PAM-CMN-5187 = ERROR: The site hardware platform is {0} ({1}), but no provision key {2} is provided.

PAM-CMN-5188 = {0}: The provision key {1} is missing for the hardware platform {2}.

PAM-CMN-5189 = Invalid provision key specified {0}. Can't have both AWS provision key and Azure provision key at the same time.

PAM-CMN-5190 = This CA PAM appliance lost the connection to the member(s) in the primary site and is in the mode only admin level users can login.

PAM-CMN-5191 = Invalid provision key specified {0}.

PAM-CMN-5192 = Resync site member failed, the member {0} is unresponsive.

PAM-CMN-5193 = Failed to load configuration from the member {0}: bad shared key.

PAM-CMN-5195 = SEVERE: Requesting a full database dump failed because the leader failed to start the cluster, aborting...

PAM-CMN-5196 = SEVERE: Requesting if the database is ready return error, aborting...

PAM-CMN-5197 = SEVERE: Credential Manager is not running!

PAM-CMN-5198 = Failed to join the cluster. {0}

PAM-CMN-5199 = The cluster configuration has been changed on {0}. Please re-download and try again.

PAM-CMN-5200 = The cluster configuration is being updated on {0} right now, please try again later.

PAM-CMN-5201 = Failed to leave the cluster. {0}

PAM-CMN-5202 = Failed to eject the member. {0}

PAM-CMN-5203 = Failed to remove the site. {0}

## Login Sessions Management Messages

PAM-CMN-1164 = Keystroke {0} Notice: {1}

PAM-CMN-1165 = Date/Time: {0} User ID : {1} User Source IP: {2} Violation on: {3} Captured Keystrokes: {4} {5}

PAM-CMN-1166 = Unauthorized attempt by user {0} to deactivate user account {1}.

PAM-CMN-1167 = A potential tampering attempt has been detected, the end-user's local system may be compromised. Account deactivated.

PAM-CMN-1168 = User {0} terminated login session of type {1} for user {2}.

PAM-CMN-1169 = Failed to terminate the {0} connection to {1} for user {2}.

PAM-CMN-1170 = User {0} terminated the {1} connection to {2} for user {3}.

PAM-CMN-1171 = Exceeded the maximum number of allowed violations. Account deactivated.

PAM-CMN-1172 = Your session has been terminated by an CA PAM administrator.

PAM-CMN-1173 = Your connection to {0} on {1} has been terminated by an CA PAM administrator.

PAM-CMN-1174 = Your account has been deactivated. See your CA PAM administrator.

PAM-CMN-1175 = Exceeded the maximum number of allowed violations. Session terminated.

PAM-CMN-1176 = A potential tampering attempt has been detected, the end-user's local system may be compromised. Session will be terminated.

PAM-CMN-1177 = Exceeded the maximum number of allowed violations but since this is a global administrator account, the account will not be deactivated.

PAM-CMN-1178 = A potential tampering attempt has been detected on your system. Your session will be terminated.

PAM-CMN-1179 = User {0} requested re-authentication for user {1}.

PAM-CMN-1180 = Invalid action or filter criteria.

PAM-CMN-1181 = Your session has been terminated. Please re-authenticate to CA PAM.

PAM-CMN-1182 = SAML session types cannot be re-authenticated.

PAM-CMN-2661 = Your session has been terminated because of concurrent login restriction.

PAM-CMN-2968 = Blocked Access to Host {0}:{1} - Blacklist policy violation.

PAM-CMN-2969 = Granted Access to Host {0}:{1} - Blacklist policy allowed host and port.

PAM-CMN-2970 = Blocked Access to Host {0}:{1} - Whitelist policy violation.

PAM-CMN-2971 = Granted Access to Host {0}:{1} - Whitelist policy allowed host and port.

PAM-CMN-2972 = A potential tampering attempt has been detected, and the end-user's local system may be compromised. Session terminated.

PAM-CMN-2973 = A potential tampering attempt has been detected, and the end-user's local system may be compromised. Account deactivated.

PAM-CMN-2974 = Possible injection attack. Invalid sessionId: {0}.

PAM-CMN-2974 = Possible injection attack. Invalid serviceName: {0}.

PAM-CMN-3169 = A malicious client may be eavesdropping on your session.

PAM-CMN-3170 = Could not grab {0}. A malicious client may be eavesdropping on your session.

PAM-CMN-3171 = Enter {0}@{1}'s old password:  
PAM-CMN-3172 = Enter {0}@{1}'s new password:  
PAM-CMN-3179 = Authentication successful  
PAM-CMN-3181 = Invalid server  
PAM-CMN-3182 = Wait for the tokencode to change, then enter the new tokencode:  
PAM-CMN-3183 = Your new PIN has been set into the system. Please wait for the tokencode to change, then authenticate again with your complete passcode now.  
PAM-CMN-3184 = Your new PIN has been rejected by the system.  
PAM-CMN-3185 = The system has generated a new PIN for you. This PIN will form the first part of your passcode. Your PIN is: {0}. Please wait for the tokencode to change, then authenticate again with your complete passcode.  
PAM-CMN-3186 = System pin rejected by the system itself  
PAM-CMN-3187 = To continue you must enter a new PIN. Enter a new PIN of {0} alphanumeric characters:  
PAM-CMN-3188 = To continue you must enter a new PIN. Enter a new PIN between {0} and {1} alphanumeric characters:  
PAM-CMN-3189 = To continue you must enter a new PIN. Enter a new PIN of {0} digits:  
PAM-CMN-3190 = To continue you must enter a new PIN. Enter a new PIN between {0} and {1} digits:  
  
PAM-CMN-3226 = Cluster orchestration updating configuration to reflect site membership update  
PAM-CMN-3232 = Saving RDP client random key failed. RDP session connection will be terminated.

## Configuration Messages

PAM-CMN-1183 = CA PAM is not provisioned with a valid license.  
PAM-CMN-1184 = CA PAM license will expire on {0,date,medium}.  
PAM-CMN-1185 = CA PAM license will expire today.  
PAM-CMN-1186 = CA PAM license has expired and access services will be disabled on {0,date,medium}. Please contact your CA Account Representative.  
PAM-CMN-1187 = CA PAM license has expired and access services are now disabled. Please contact your CA Account Representative.  
PAM-CMN-1188 = Version value not numeric.  
PAM-CMN-1189 = Hardware ID not a string.  
PAM-CMN-1190 = Access license not an integer.  
PAM-CMN-1191 = Password license not an integer.  
PAM-CMN-1192 = A2A license not an integer.  
PAM-CMN-1193 = Invalid value for mainframe license.  
PAM-CMN-1194 = Invalid value for AWS license.  
PAM-CMN-1195 = Invalid value for perpetual license.  
PAM-CMN-1196 = Invalid value for start date.  
PAM-CMN-1197 = Invalid value for end date.  
PAM-CMN-1198 = Invalid value for spike license.  
PAM-CMN-1199 = Invalid value for evaluation license.  
PAM-CMN-1200 = Start date is in the future.  
PAM-CMN-1201 = End date is greater than start date.  
PAM-CMN-1202 = End date is in the past.  
PAM-CMN-1203 = End date required but not specified.  
PAM-CMN-1204 = Updated license.  
PAM-CMN-1205 = Insufficient permissions to update license.  
PAM-CMN-1206 = Insufficient permissions to set hardware serial.  
PAM-CMN-1207 = License file contains invalid parameters  
PAM-CMN-1208 = Hardware ID in the license does not match the appliance.  
PAM-CMN-1209 = There are more CA PAM devices than this license permits.

PAM-CMN-1210 = There are more Password devices than this license permits.

PAM-CMN-1211 = There are more A2A devices than this license permits.

PAM-CMN-1212 = New license does not permit AWS. Clear your AWS configuration before continuing.

PAM-CMN-1213 = New license does not permit mainframe access. Remove existing mainframe Access Methods before continuing.

PAM-CMN-1214 = CA PAM license is invalid and access services are now disabled. Please contact your CA Account Representative.

PAM-CMN-1215 = AWS license requires Access and Password license nodes.

PAM-CMN-1216 = The license was not updated. There was a failure deleting the Office365 device. See the audit log for more details.

PAM-CMN-1217 = The license was not updated. There was an error provisioning the Office365 device. See the audit log for more details.

PAM-CMN-1218 = The license was not updated. There was a failure deleting the AWS device. See the audit log for more details.

PAM-CMN-1219 = The license was not updated. There was an error provisioning the AWS device. See the audit log for more details.

PAM-CMN-1220 = New license does not permit Office365. Clear your Office365 configuration before continuing.

PAM-CMN-1221 = There are more AWS Proxy users than this license permits.

PAM-CMN-1222 = AWS Proxy license requires Access, Password, and A2A nodes.

PAM-CMN-1223 = CA PAM evaluation license will expire today.

PAM-CMN-1224 = CA PAM evaluation license has expired and access services will be disabled on {0,date,medium}. Please contact your CA Account Representative.

PAM-CMN-1225 = CA PAM evaluation license has expired and access services are now disabled. Please contact your CA Account Representative.

PAM-CMN-1226 = Spike (temporary) CA PAM license will expire on {0,date,medium}.

PAM-CMN-1227 = Spike CA PAM license will expire today.

PAM-CMN-1228 = Spike CA PAM license has expired and access services will be disabled on {0,date,medium}. Please contact your CA Account Representative.

PAM-CMN-1229 = Spike CA PAM license has expired and access services are now disabled. Please contact your CA Account Representative.

PAM-CMN-1230 = CA PAM license is invalid: {0}

PAM-CMN-1231 = New license does not permit VMware. Clear your VMware configuration before continuing.

PAM-CMN-1232 = VMware license requires at least one PA license node.

PAM-CMN-1233 = The license was not updated. There was an error creating the NSX service. See the audit log for more details.

PAM-CMN-1234 = The license was not updated. There was a failure deleting the NSX service. See the audit log for more details.

PAM-CMN-1235 = There are more NSX Proxy users than this license permits.

PAM-CMN-1236 = Your connection to '{0}'{1} has been terminated by VMware NSX Security Policy.

PAM-CMN-1237 = The license was not updated. NSX Proxy License requires VMware license

PAM-CMN-1238 = Invalid license file

PAM-CMN-1239 = Invalid start date

PAM-CMN-1240 = Invalid end date

PAM-CMN-1241 = Start date in the future.

PAM-CMN-1242 = More CA PAM Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-1243 = More Password Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-1244 = More A2A Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-1245 = AWS capabilities in use, but not permitted by license.

PAM-CMN-1246 = Mainframe access method policies found, but not permitted by license.

PAM-CMN-1247 = Unable to determine license type.

PAM-CMN-1248 = VMware capabilities in use, but not permitted by license.

PAM-CMN-1249 = Office365 capabilities in use, but not permitted by license.

PAM-CMN-1250 = AWS API Proxy license not an integer.

PAM-CMN-1251 = AWS API Proxy license cannot be removed. There are {0} user(s) with the AwsApiProxy privilege.

PAM-CMN-1252 = AWS API Proxy capabilities in use, but not permitted by license.

PAM-CMN-1253 = Failed to update AWS API Proxy whitelist: {0}.

PAM-CMN-1254 = Invalid action issued to AWS API Proxy whitelist: {0}.

PAM-CMN-1255 = Invalid subnet {0}. Format should be in CIDR notation (xxx.xxx.xxx.xxx/xx).

PAM-CMN-1256 = HSM capabilities in use, but not permitted by license.

PAM-CMN-1257 = Invalid permission to activate admin mode.

PAM-CMN-1258 = Web SSO not enabled.

PAM-CMN-1259 = SafeNet HSM must be removed before Entrust HSM may be licensed.

PAM-CMN-1260 = Entrust HSM must be removed before SafeNet HSM may be licensed.

PAM-CMN-1261 = Only one type of HSM (SafeNet, Entrust) may be specified in a license.

PAM-CMN-1262 = The license was not updated. There was a failure setting up VMware. See the audit log for more details.

PAM-CMN-1263 = The license was not updated. There was a failure shutting down VMware. See the audit log for more details.

PAM-CMN-1264 = Upgrade failed. Please review the audit log and then perform a system recovery.

PAM-CMN-1265 = Failed to install API key infrastructure. Please check the logs to find the problem and reapply the license.

PAM-CMN-1266 = The license was not updated. External API feature was not added. Please check the logs to find the problem and reapply the license.

PAM-CMN-1267 = The license was not updated. External API feature not removed. Existing client API keys may need to be deleted.

PAM-CMN-1268 = Invalid value for External API license.

PAM-CMN-1269 = Failed to update Proxy whitelist: {0}.

PAM-CMN-1270 = Invalid action issued to Proxy whitelist: {0}.

PAM-CMN-1271 = Invalid subnet {0}. Format should be in CIDR notation (xxx.xxx.xxx.xxx/xx).

PAM-CMN-1272 = AWS Proxy Account cannot be generated. There are more AWS proxy accounts than license permits

PAM-CMN-1273 = NSX Proxy Account cannot be generated. There are more NSX proxy accounts than license permits

PAM-CMN-1274 = The license was not updated. Uploaded license file could not be verified or read.

PAM-CMN-1275 = CA Threat Analytics license requires that External API also be licensed.

PAM-CMN-1276 = The CA Threat Analytics special user is deleted when the CA Threat Analytics is no longer licensed, and may not be deleted otherwise.

PAM-CMN-1277 = Invalid value for CA Threat Analytics license.

PAM-CMN-1278 = The license was not updated. CA Threat Analytics feature was not added. Please check the logs to find the problem and reapply the license.

PAM-CMN-1279 = The license was not updated. CA Threat Analytics feature not removed. Please check the logs to find the problem and reapply the license.

PAM-CMN-2016 = CA PAM license is invalid: CA PAM is not provisioned with a valid license.

PAM-CMN-2017 = CA PAM license is invalid: Invalid license file

PAM-CMN-2018 = CA PAM license is invalid: Invalid start date

PAM-CMN-2019 = CA PAM license is invalid: Invalid end date

PAM-CMN-2020 = CA PAM license is invalid: Start date in the future.

PAM-CMN-2021 = CA PAM license is invalid: More CA PAM Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-2022 = CA PAM license is invalid: More Password Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-2023 = CA PAM license is invalid: More A2A Devices are provisioned than are permitted by this CA PAM license.

PAM-CMN-2024 = CA PAM license is invalid: AWS capabilities in use, but not permitted by license.

PAM-CMN-2025 = CA PAM license is invalid: AWS API Proxy capabilities in use, but not permitted by license.

PAM-CMN-2026 = CA PAM license is invalid: VMware capabilities in use, but not permitted by license.

PAM-CMN-2027 = CA PAM license is invalid: Office365 capabilities in use, but not permitted by license.



PAM-CMN-2028 = CA PAM license is invalid: HSM capabilities in use, but not permitted by license.  
 PAM-CMN-2029 = CA PAM license is invalid: Only one type of HSM (SafeNet, Entrust) may be specified in a license.  
 PAM-CMN-2030 = CA PAM license is invalid: Mainframe access method policies found, but not permitted by license.  
 PAM-CMN-2031 = CA PAM license is invalid: Unable to determine license type.  
 PAM-CMN-3348 = CA PAM license is invalid: Sailpoint Table Integration is installed, but not permitted by license.  
 PAM-CMN-3400 = NSX Proxy license requires Access, Password, and A2A nodes.  
 PAM-CMN-3401 = NSX API Proxy license cannot be removed. There are {0} users with the NsxApiProxy privilege.  
 PAM-CMN-3402 = NSX API Proxy license is not an integer.  
 PAM-CMN-3403 = The interval between emails is required.  
 PAM-CMN-3404 = NSX Proxy service can not be deleted.  
 PAM-CMN-3405 = Invalid role type: {0}.  
 PAM-CMN-3328 = Group code {0} is not allowed.  
 PAM-CMN-3329 = Group code is required.  
 PAM-CMN-3330 = Group code may not be updated.  
 PAM-CMN-4816 = Invalid value for SailPoint.  
 PAM-CMN-5191 = Invalid provision key specified {0}.  
 PAM-CM-5200=PAM-CM-5200: Email successfully sent to the SMTP server {0}. Please verify if the email was delivered to the recipient at {1}.  
 PAM-CM-5201=PAM-CM-5201: {0}. See diagnostic logs for details.

## HSM Configuration Messages

PAM-CMN-1256 = HSM capabilities in use, but not permitted by license.  
 PAM-CMN-1259 = SafeNet HSM must be removed before Entrust HSM may be licensed.  
 PAM-CMN-1260 = Entrust HSM must be removed before SafeNet HSM may be licensed.  
 PAM-CMN-1261 = Only one type of HSM (SafeNet, Entrust) may be specified in a license.  
 PAM-CMN-1280 = CA PAM is not provisioned to use an HSM  
 PAM-CMN-1281 = Error trying to provision CA PAM for SafeNet HSM.  
 PAM-CMN-1282 = SafeNet HSM with address {0} added.  
 PAM-CMN-1283 = Attempt to remove the SafeNet HSM configuration failed due to the passwords currently being re-encrypted  
 PAM-CMN-1284 = HSM with address {0} removed.  
 PAM-CMN-1285 = Attempt to initialize LUNA PCI has failed  
 PAM-CMN-1286 = LUNA PCI has been initialized successfully  
 PAM-CMN-1287 = Attempt to activate LUNA PCI has failed  
 PAM-CMN-1288 = LUNA PCI has been activated  
 PAM-CMN-1289 = Attempt to extract LUNA PCI Key has failed  
 PAM-CMN-1290 = LUNA PCI Key extracted  
 PAM-CMN-1291 = Failed to securely insert the cipher key  
 PAM-CMN-1292 = Success inserting the encrypted cipher key into the LunaPCI-E device  
 PAM-CMN-1293 = Failed to initialize the internal LunaPCI-E device  
 PAM-CMN-1294 = Failed to create a partition on the internal LunaPCI-E device  
 PAM-CMN-1295 = Success initializing the internal LunaPCI-E device  
 PAM-CMN-1296 = Failed to securely extract the cipher key  
 PAM-CMN-1297 = Failed to PED activate the LunaPCI-E partition  
 PAM-CMN-1298 = Failed to secure the partition password for the LunaPCI-E partition  
 PAM-CMN-1299 = Failed to log into the partition with the supplied password  
 PAM-CMN-1300 = Failed to generate the cypher key during the initial activation  
 PAM-CMN-1301 = Success activating the LunaPCI-E device on this non primary clustered CA PAM

PAM-CMN-1302 = Success activating the LunaPCI-E device on this primary clustered CA PAM  
PAM-CMN-1303 = Success activating the LunaPCI-E device on this standalone CA PAM...reboot is needed  
PAM-CMN-1304 = Error HSM script arguments are incomplete  
PAM-CMN-1305 = Error CA PAM is not configured to use an HSM  
PAM-CMN-1306 = Error the HSM password is incorrect  
PAM-CMN-1307 = Success updating the HSM password

PAM-CMN-2547 = Cannot add a networked HSM because this PAM has an internal LunaPCI-E device  
PAM-CMN-2548 = Proper usage: addHSM <input\_1> <input\_2> <input\_3> <input\_4> <input\_5> <input\_6>  
PAM-CMN-2549 = The HSM software is not installed on PAM

PAM-CMN-2806 = Proper usage: appendHSM <principalName> <HSM\_IP> <principalPassword> <storagePassword>  
<storageName>

PAM-CMN-2808 = The partition {0} on the first HSM does not match with {1} on this HSM  
PAM-CMN-2809 = PAM is not provisioned to use an HSM. Please install the first HSM.  
PAM-CMN-2810 = The HSM group is already at the maximum of 3  
PAM-CMN-2811 = Cannot determine the primary HSM group member.  
PAM-CMN-2812 = The HSM {0} is already provisioned on this PAM  
PAM-CMN-2813 = Cannot determine the HSM group members.

PAM-CMN-2815 = Unable to copy the HSM certificate

PAM-CMN-2817 = This client {0} is already registered on the HSM

PAM-CMN-2820 = Failed to add HSM {0}. Consistency check failed  
PAM-CMN-2821 = Failed to add HSM {0}. Post synch consistency check failed  
PAM-CMN-2822 = Success, you must reboot the appliance for this change to take effect!  
PAM-CMN-2823 = Proper usage: appendThalesHSM <tokenName> <RFS\_IP> <HSM\_IP> <tokenPassword>  
PAM-CMN-2824 = Cannot deploy an OCS with individual names. All cards in the OCS must be named the same and must have the same passwords.

PAM-CMN-2825 = Bad HSM IP address  
PAM-CMN-2826 = Bad RFS IP address  
PAM-CMN-2827 = Failed to get the ESN and hash from {0}  
PAM-CMN-2828 = Failed to enroll the client to the HSM {0}  
PAM-CMN-2829 = Proper usage: createHSM <principalName> <HSM\_IP> <principalPassword> <storagePassword>  
<storageName>

PAM-CMN-2830 = PAM is already provisioned to use an HSM

PAM-CMN-2833 = Invalid Security Principal, Password or HSM IP address. Please try again.

PAM-CMN-2835 = Unable to create a Luna client certificate  
PAM-CMN-2836 = HSM connection test from {0} failed.

PAM-CMN-2839 = PAM is not provisioned to use an HSM  
PAM-CMN-2840 = Failed to remove HSM {0}  
PAM-CMN-2841 = {0} is not a deployed HSM.  
PAM-CMN-2842 = Unknown HSM vendor  
PAM-CMN-2843 = Cannot mix HSMs from different vendors  
PAM-CMN-2844 = Proper usage: removeHSM <HSM\_IP>  
PAM-CMN-2845 = The HSM {0} is not provisioned on this PAM  
PAM-CMN-2846 = LunaPCI-E Uninitialized  
PAM-CMN-2847 = LunaPCI-E Initialized

PAM-CMN-2850="PAM is currently provisioned to use an HSM"

PAM-CMN-2866 = Proper usage: createThalesHSM <tokenName> <RFS\_IP> <HSM\_IP> <tokenPassword>  
PAM-CMN-2867 = Failed to get the ESN and hash from {0} on port {1}

PAM-CMN-2868 = Failed to setup with the RFS {0} on port {1}  
 PAM-CMN-2869 = Failed to synch update with the RFS {0} on port {1}  
 PAM-CMN-2870 = Failed to test login cache with the HSM token {0}  
 PAM-CMN-2871 = Failed to test login with the HSM token {0}  
 PAM-CMN-2872 = Failed to generate the AES256 cipher key on the HSM token {0}  
 PAM-CMN-2873 = This standalone PAM does not have commit permission to the RFS. You must run 'rfs-setup --gang-client' on the RFS first.  
 PAM-CMN-2875 = Failed to get the ESN and hash from {0}  
 PAM-CMN-3234="The HSM is not functioning properly with PKCS11 result: {0}, {1}"

## Secondary Transparent Login Messages

PAM-CMN-1308 = Transparent Login Configuration name is empty.  
 PAM-CMN-1309 = Transparent Login Configuration invalid. See log for details.  
 PAM-CMN-1310 = Transparent Login Configuration name cannot be longer than 128 characters.  
 PAM-CMN-1311 = XML for Transparent Login Configuration invalid.  
 PAM-CMN-1312 = Transparent Login Configuration not found.  
 PAM-CMN-1313 = Transparent Login Configuration name {0} must be unique.  
 PAM-CMN-1314 = The given Transparent Login Configuration is used by one or several RDP applications.  
 PAM-CMN-1315 = Hide from user is required.  
 PAM-CMN-1316 = Transparent Login Enabled is required.  
 PAM-CMN-1317 = Invalid data 'Hide From User'.  
 PAM-CMN-1318 = Invalid data 'Transparent Login Enabled'.  
 PAM-CMN-1319 = Transparent Login window is required.  
 PAM-CMN-1320 = Invalid Transparent Login Window.  
 PAM-CMN-1321 = Application Fingerprint must consist of 128 characters.  
 PAM-CMN-1322 = Invalid Application Fingerprint. Only the following characters are allowed for fingerprint: 0-9 A-F.  
 PAM-CMN-1323 = Transparent Login Configurations for RDP Application {0} do not exist, or the Transparent Login section contains invalid data (Window Titles: {1}).  
 PAM-CMN-1324 = Transparent Login Window with the title '{0}' already exists for this RDP application.  
 PAM-CMN-1325 = Login failed for user {0} due to multiple active TACACS+ users having the same login name. All TACACS+ users with login name {1} will be deactivated.  
 PAM-CMN-1326 = Login Failed. Please contact your system administrator for further assistance.  
 PAM-CMN-1327 = TACACS+ user {0} moved from TACACS+ group {1} to TACACS+ group {2}.  
 PAM-CMN-1328 = Authentication failed for TACACS+ user {0}. TACACS+ authentication succeeded but the user's TACACS+ group changed from {1} to {2}. The new TACACS+ group is not registered with CA PAM. User account deleted.  
 PAM-CMN-1329 = TACACS+ user is not registered. Contact your CA PAM Administrator.  
 PAM-CMN-1330 = Authentication failed for TACACS+ user {0}. TACACS+ authentication succeeded but unable to retrieve the user's TACACS+ group.

## AWS, VMware, and Azure Virtual Device Management Messages

PAM-CMN-1331 = Duplicate {0} Provision is not allowed.  
 PAM-CMN-1332 = Unable to retrieve AWS proxy account. Please contact CA PAM administrator.  
 PAM-CMN-1333 = Unable to retrieve NSX proxy account. Please contact CA PAM administrator.  
 PAM-CMN-1334 = There was an error during proxy account deletion.  
 PAM-CMN-1438 = Unauthorized attempt to save VMware NSX configuration  
 PAM-CMN-1439 = Unauthorized attempt to clear VMware NSX configuration  
 PAM-CMN-1440 = Unauthorized attempt to retrieve VMware NSX configuration  
 PAM-CMN-1441 = Certificate info of VMware NSX Service Manager was successfully updated.



PAM-CMN-1442 = Failed to update certificate info of VMware NSX Service Manager.  
PAM-CMN-1443 = PAM Service was successfully registered in VMware NSX Manager with URL {0}.  
PAM-CMN-1444 = Failed to registered PAM Service in VMware NSX Manager with URL {0}.  
PAM-CMN-1445 = PAM Service was successfully unregistered from VMware NSX Manager with URL {0}.  
PAM-CMN-1446 = VMware NSX configuration ({0}) was successfully cleared.  
PAM-CMN-1447 = VMware NSX configuration was cleared but PAM Service was not unregistered from VMware NSX Manager with URL {0}.  
PAM-CMN-1448 = Failed to unregister PAM Service from VMware NSX Manager with URL {0}.  
  
PAM-CMN-1507 = Failed to connect to AWS Access key {0}. Code: {1}, Reason: {2}.  
PAM-CMN-1508 = Unauthorized attempt to purge all AWS virtual devices  
PAM-CMN-1509 = Unauthorized attempt to create AWS provision type  
  
PAM-CMN-1547 = Device {0} was provisioned by another VMware user and was not updated  
  
PAM-CMN-1550 = Connection to '{0}' has been terminated by VMware NSX Security Policy  
  
PAM-CMN-1591 = Unauthorized attempt to purge all VMware virtual devices  
PAM-CMN-1592 = {0} VMware devices were not deleted. Credentials are kept and the connection was set to inactive.  
PAM-CMN-1593 = All VMware virtual devices were deleted  
PAM-CMN-1594 = Unauthorized attempt to create VMware provision type  
PAM-CMN-1595 = Unauthorized attempt to clear VMware provision type  
PAM-CMN-1596 = Unauthorized attempt to add VMware provision key.  
PAM-CMN-1597 = Synchronization of security tags and groups with VMware NSX was not done.  
PAM-CMN-1598 = Synchronization of security tags and groups with VMware NSX completed successfully.  
  
PAM-CMN-1649 = Unable to retrieve the AWS Virtual Management IP provision region. The VIP cannot be managed on this node.  
  
PAM-CMN-1652 = There was an error retrieving credentials for AWS  
PAM-CMN-1653 = Unable to retrieve the AWS Virtual Management IP provision key. The VIP cannot be managed on this node.  
  
PAM-CMN-1657 = Unable to retrieve AWS secret key for use by S3 storage.  
  
PAM-CMN-1712 = No source IP address found for AWS API Proxy request.  
PAM-CMN-1713 = Invalid source IP address {0} found for AWS API Proxy request.  
PAM-CMN-1714 = AWS API Proxy request came from IP address {0}, which is not on any whitelist.  
PAM-CMN-1715 = AWS API Proxy request for user {0} failed due to authentication failure. See previous log messages for details.  
PAM-CMN-1716 = Completely unexpected result was returned for Authentication Service for AWS proxy login. Returned value was {0}  
PAM-CMN-1717 = AWS API Proxy user {0} was not logged in because they do not have the AWS API Proxy user privilege  
PAM-CMN-1719 = Problems communicating with AWS. Message was {0}  
PAM-CMN-1746 = Added AWS policy {0}  
  
PAM-CMN-1748 = Updated AWS policy {0}  
PAM-CMN-1749 = Deleted AWS policy {0}  
  
PAM-CMN-1751 = Unable to find AWS device by its device id  
PAM-CMN-1752 = Unknown EC2 Region code {0}. Region will not be set.  
PAM-CMN-1753 = Unable to open AWS provisioning lock file  
PAM-CMN-1754 = AWS provisioning already in progress.  
PAM-CMN-1755 = Failed to connect to AWS. Exception was {0}  
PAM-CMN-1756 = Unknown AWS region code {0}  
PAM-CMN-1757 = Cannot allow delete of access pair {0} as it is used for AWS provisioning in region {1}  
PAM-CMN-1758 = Cannot allow delete of access pair {0} because it is used to access the AWS Management console by {1} {2}

PAM-CMN-1766 = Device Group {0} is not added to VMware

PAM-CMN-1778 = Unexpected return from viewAccountPassword. Connection to VMware vCenter/NSX aborted.

PAM-CMN-1779 = Invalid VMware Configuration - invalid URL {0}

PAM-CMN-1780 = Unable to open VMWARE provisioning lock file

PAM-CMN-1781 = Failed to connect to VMware using URL {0} for user {1}.

PAM-CMN-1782 = Invalid data returned from VMware at {0} for user {1}. Data was {2}.

PAM-CMN-1783 = VMware provisioning already in progress at {0} for user {1}.

PAM-CMN-1784 = Error when attempting to create NSX device - error was {0}

PAM-CMN-1785 = No source IP address found for NSX API Proxy request.

PAM-CMN-1786 = Invalid source IP address {0} found for NSX API Proxy request.

PAM-CMN-1787 = VMware NSX API Proxy request for user {0} failed due to authentication failure. See previous log messages for details.

PAM-CMN-1788 = Completely unexpected result was returned for Authentication Service for VMware NSX proxy login. Returned value was {0}

PAM-CMN-1789 = VMware NSX API Proxy user {0} was not logged in because they do not have the VMware NSX API Proxy user privilege

PAM-CMN-1803 = Unable to find master target aws credential - request aborted

PAM-CMN-1813 = No user name supplied for AWS Management console.

PAM-CMN-1814 = No AWS URL was generated for policy {0} using user friendly account name {1}

PAM-CMN-1817 = Missing owner on NSX Proxy account {0}

PAM-CMN-1819 = Added {0} to AWS API Proxy Auto-Activation Whitelist.

PAM-CMN-1820 = Removed {0} from AWS API Proxy Auto-Activation Whitelist.

PAM-CMN-1821 = Added {0} to VMware NSX API Proxy Auto-Activation Whitelist.

PAM-CMN-1822 = Removed {0} from VMware NSX API Proxy Auto-Activation Whitelist.

PAM-CMN-1824 = Error when attempting to create NSX proxy account - unable to get PA user ID for user

PAM-CMN-1825 = Error when attempting to create AWS proxy account - unable to get PA user ID for user

PAM-CMN-1826 = Missing owner on AWS Proxy account {0}

PAM-CMN-1837 = Missing required AWS getProxyToken parameter user name

PAM-CMN-1838 = Missing required AWS getProxyToken parameter password

PAM-CMN-1839 = Missing required AWS getProxyToken parameter user name, password

PAM-CMN-1840 = Missing the following required attributes to get an AssumeRole token: AWS policy.

PAM-CMN-1841 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key.

PAM-CMN-1842 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, Secret key.

PAM-CMN-1843 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, Secret key, ARN ID.

PAM-CMN-1844 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, Secret key, ARN ID, Target account user name.

PAM-CMN-1845 = Missing the following required attributes to get an AssumeRole token: AWS policy, Secret key.

PAM-CMN-1846 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, ARN ID.

PAM-CMN-1847 = Missing the following required attributes to get an AssumeRole token: AWS policy, Secret key, ARN ID.

PAM-CMN-1848 = Missing the following required attributes to get an AssumeRole token: AWS policy, Secret key, Target account user name.

PAM-CMN-1849 = Missing the following required attributes to get an AssumeRole token: AWS policy, ARN ID, Target account user name.

PAM-CMN-1850 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, Target account user name.

PAM-CMN-1851 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, ARN ID, Target account user name.

PAM-CMN-1852 = Missing the following required attributes to get an AssumeRole token: AWS policy, Secret key, ARN ID, Target account user name.

PAM-CMN-1853 = Missing the following required attributes to get an AssumeRole token: AWS policy, ARN ID

PAM-CMN-1854 = Missing the following required attributes to get an AssumeRole token: AWS policy, Target account user name

PAM-CMN-1855 = Failed to find AWS access key

PAM-CMN-1856 = Failed to find AWS secret key

PAM-CMN-1857 = Failed to find AWS access key and AWS secret key

PAM-CMN-1858 = VMware configuration missing fields: VMware user name, VMware password, VMware URL.

PAM-CMN-1859 = VMware configuration missing fields: VMware user name.

PAM-CMN-1860 = VMware configuration missing fields: VMware password.

PAM-CMN-1861 = VMware configuration missing fields: VMware URL.

PAM-CMN-1862 = VMware configuration missing fields: VMware user name, VMware password.

PAM-CMN-1863 = VMware configuration missing fields: VMware user name, VMware URL.

PAM-CMN-1864 = VMware configuration missing fields: VMware password, VMware URL.

PAM-CMN-1865 = Missing required NSX getProxyToken parameters user name, password.

PAM-CMN-1866 = Missing required NSX getProxyToken parameters user name.

PAM-CMN-1867 = Missing required NSX getProxyToken parameters password.

PAM-CMN-1878 = {0} total AWS devices were not deleted. Provisioning information is kept and the connection was set to inactive.

PAM-CMN-1879 = All AWS virtual devices were deleted

PAM-CMN-1882 = Provisioning information and AWS devices for access {0} and region {1} deleted.

PAM-CMN-1883 = {0} AWS devices were not deleted for access code and region {1}. Credentials are kept and the connection was set to inactive.

PAM-CMN-1884 = AWS provisioning added for access key {0} in region {1}. Active state is {2}

PAM-CMN-1886 = Updated AWS refresh interval to {0}.

PAM-CMN-1893 = All VMware provisionings were deleted

PAM-CMN-1894 = All {0} VMware provisionings were deleted

PAM-CMN-1895 = Unable to retrieve target account information for VMware provision with URL {0}.

PAM-CMN-1896 = Provisioning information and VMware devices for vCenter URL {0} and user {1} deleted.

PAM-CMN-1897 = Update of target account {0} for device {1} failed - the account must be deleted before the device can be.

PAM-CMN-1898 = {0} VMware devices were not deleted for vCenter URL {1} and user {2}. Credentials are kept and the connection was set to inactive.

PAM-CMN-1899 = Add VMware provisioning row, but unable to retrieve account name or device name

PAM-CMN-1900 = Added VMware provisioning for vCenter URL {0} and user {1}.

PAM-CMN-1901 = Updated VMware provisioning for {0} user {1} to URL {2} active = {3}

PAM-CMN-1902 = Activated VMware provisioning for vCenter URL {0} but unable to retrieve account name or device name.

PAM-CMN-1903 = Deactivated VMware provisioning for vCenter URL {0} but unable to retrieve account name or device name.

PAM-CMN-1904 = Activated VMware provisioning for vCenter URL {0} and user {1}.

PAM-CMN-1905 = Deactivated VMware provisioning for vCenter URL {0} and user {1}.

PAM-CMN-1906 = Activated all VMware provisioning. {0} were not yet activated.

PAM-CMN-1907 = Deactivated all VMware provisioning. {0} were not yet deactivated.

PAM-CMN-1909 = Updated VMware refresh interval to {0}

PAM-CMN-1943 = Missing the following required attributes to get an AssumeRole token: AWS policy, Access key, Secret key, Target account user name.

PAM-CMN-1944 = Missing the following required attributes to get an AssumeRole token: Access key.

PAM-CMN-1945 = Missing the following required attributes to get an AssumeRole token: Access key, Secret key.

PAM-CMN-1946 = Missing the following required attributes to get an AssumeRole token: Access key, Secret key, ARN ID.

PAM-CMN-1947 = Missing the following required attributes to get an AssumeRole token: Access key, Secret key, Target account user name.

PAM-CMN-1948 = Missing the following required attributes to get an AssumeRole token: Access key, Secret key, ARN ID, Target account user name.

PAM-CMN-1949 = Missing the following required attributes to get an AssumeRole token: Secret key.

PAM-CMN-1950 = Missing the following required attributes to get an AssumeRole token: Access key, ARN ID.

PAM-CMN-1951 = Missing the following required attributes to get an AssumeRole token: Secret key, ARN ID.

PAM-CMN-1952 = Missing the following required attributes to get an AssumeRole token: Secret key, Target account user name.

PAM-CMN-1953 = Missing the following required attributes to get an AssumeRole token: ARN ID, Target account user name.

PAM-CMN-1954 = Missing the following required attributes to get an AssumeRole token: Access key, Target account user name.

PAM-CMN-1955 = Missing the following required attributes to get an AssumeRole token: Access key, ARN ID, Target account user name.

PAM-CMN-1956 = Missing the following required attributes to get an AssumeRole token: Secret key, ARN ID, Target account user name.

PAM-CMN-1957 = Missing the following required attributes to get an AssumeRole token: ARN ID

PAM-CMN-1958 = Missing the following required attributes to get an AssumeRole token: Target account user name

PAM-CMN-2132 = type = {0}; access = {1}; password = {2}; a2a = {3}; awsAPIProxy = {4}; start = {5,date,medium} {6}

PAM-CMN-2133 = type = {0}; access = {1}; password = {2}; a2a = {3}; awsAPIProxy = {4}; start = {5,date,medium} {6} end={7,date,medium};

PAM-CMN-2226 = Unable to contact AWS Management Console for run time update. Connection aborted.

PAM-CMN-2227 = Unable to contact AWS Management Console for run time update. Attempting to connect anyway.

PAM-CMN-2228 = Master AWS Target Server. All EC2 target accounts should be associated with this device.

PAM-CMN-2276 = Unexpected PA failure on isAWSTargetType message was {0}.

PAM-CMN-2280 = Unable to calculate AWS URL for policy {0} using user friendly account name {1} - error was {2}.

PAM-CMN-2281 = Unable to calculate AWS URL - error was {0}.

PAM-CMN-2313 = Error when attempting to create NSX proxy account - error was {0}.

PAM-CMN-2314 = Error when attempting to retrieve NSX account name - error was {0}.

PAM-CMN-2315 = Error when attempting to create AWS proxy account - error was {0}.

PAM-CMN-2316 = Error when attempting to retrieve AWS account name - error was {0}.

PAM-CMN-2317 = Unable to retrieve AWS Proxy Accounts - error was {0}.

PAM-CMN-2354 = Unable to retrieve NSX Accounts. Error was {0}

PAM-CMN-2492 = Unable to contact AWS Management Console for run time update.

PAM-CMN-2493 = Unable to contact AWS Management Console for run time update. Connection aborted.

PAM-CMN-2494 = Unable to contact AWS Management Console for run time update. Attempting to connect anyway.

PAM-CMN-3237 = The AWS secret key for use by S3 storage is missing.

PAM-CMN-5350 = Azure target account is required.

PAM-CMN-5351 = Azure subscription ID is required.

PAM-CMN-5352 = The license was not updated. There was a failure deleting the Azure device. See the audit log for more details.

PAM-CMN-5353 = Updated Azure refresh interval to {0}.

PAM-CMN-5354 = Unauthorized attempt to create Azure provision type

PAM-CMN-5355 = Unable to find AWS device by its device id

PAM-CMN-5356 = Unable to contact Azure Active Directory for run time update. Connection aborted.  
 PAM-CMN-5357 = Unable to contact Azure Active Directory for run time update. Attempting to connect anyway.  
 PAM-CMN-5358 = Unable to contact Azure Active Directory for run time update.  
 PAM-CMN-5359 = This subscription and resource group are already provisioned.  
 PAM-CMN-5360 = Failed to get Azure API access token.  
 PAM-CMN-5361 = Failed to access Azure API.  
 PAM-CMN-5362 = Azure provisioning added for target account {0} subscription {1} and resource group {2}. Active state is {3}  
 PAM-CMN-5363 = Provisioning information and Azure devices for subscription {0} and resource group {1} deleted.  
 PAM-CMN-5364 = {0} Azure devices were not deleted for subscription {1}. The connection was set to inactive.  
 PAM-CMN-5365 = {0} Azure devices were not deleted. See logs for details. The configuration is now inactive.  
 PAM-CMN-5366 = Target account restrict delete was not set for provision row for target account {0} subscription {1}: {2}  
 PAM-CMN-5367 = Unable to retrieve Azure Accounts. Error was {0}  
 PAM-CMN-5368 = Unable to retrieve Azure account. Please contact CA PAM administrator.  
 PAM-CMN-5369 = Unable to retrieve Azure target application. Please contact CA PAM administrator.  
 PAM-CMN-5370 = Unable to find master target azure credential - request aborted  
 PAM-CMN-5371 = Azure provisioning request  
 PAM-CMN-5372 = Device imported from Azure  
 PAM-CMN-5373 = Microsoft Azure Target Server. All Azure target accounts should be associated with this device.  
 PAM-CMN-5374 = Azure Users sync completed: {0} Azure users deleted, {1} Azure users remaining.  
 PAM-CMN-5375 = User {0} deleted from Azure. Deleting user ...  
 PAM-CMN-5376 = Azure provisioning updated for target account {0} subscription {1} and resource group {2}. User sync state is {3} and Device sync state is {4}  
 PAM-CMN-5377 = The User Sync checkbox must have a value of t or f.  
 PAM-CMN-5378 = The Device Sync checkbox must have a value of t or f.  
 PAM-CMN-5379 = Azure users deprovision failed. Error getting Resource Id from Azure.  
 PAM-CMN-5380 = Azure user {0} unassigned from CA PAM Azure App. Deleting user ...  
 PAM-CMN-5381 = Updated Azure devices refresh interval to {0}.  
 PAM-CMN-5382 = Updated Azure users refresh interval to {0}.  
 PAM-CMN-5383 = Unable to retrieve Azure VIP provision configuration. Please make sure Azure connection has been setup properly under PAM Configuration.  
 PAM-CMN-5384 = Unable to retrieve Azure VIP provision account details. Perhaps PA is restarting or down?  
 PAM-CMN-5385 = Unable to retrieve Azure VIP provision account password. Perhaps PA is restarting or down?  
 PAM-CMN-5386 = Failed to update Azure network interface - private IP {0} - public IP {1}. Error: {2}  
 PAM-CMN-5387 = Failed to get Azure IP configuration status - {0}

## Credential Management API Non-Device Messages

PAM-CMN-1335 = Role description may not be longer than 100 characters.  
 PAM-CMN-1336 = Invalid target account id {0} specified.  
 PAM-CMN-1337 = Invalid target application id specified.  
 PAM-CMN-1338 = The password request failed: {0}  
 PAM-CMN-1339 = Invalid type {0} for listing password view requests.  
 PAM-CMN-3288 = Allows the use of the External API by {0}.  
 PAM-CMN-3289 = All the privileges needed for {0} to use the external API.  
 PAM-CMN-3290 = Allows the user to use the AWS API Proxy.  
 PAM-CMN-3291 = Allows the user to log in, check the access page, and remotely access the AWS API Proxy



PAM-CMN-3292 = Allows the user to use the VMware NSX API Proxy.

PAM-CMN-3293 = Allows the user to log in, check the access page, and remotely access the VMware NSX API Proxy

## Session Recording Messages

PAM-CMN-1340 = Session recording mount not available. The reconciliation process was not launched.

PAM-CMN-1384 = Session recording flag file ksl\_logfile restored. CLI recording flag was {0}. Graphical recording flag was {1}.

PAM-CMN-1385 = Syslog recording flag file ksl\_sylog restored. Syslog recording flag was {0}.

PAM-CMN-1503 = Updated Session Recording to be Security Safe

PAM-CMN-1504 = Updated Session Recording to be Operationally Safe

PAM-CMN-1549 = Session recording purging settings updated.

PAM-CMN-1747 = Session recording '{0}' was viewed

PAM-CMN-1880 = Cannot delete - used for storing session recording logs. Change the provision row used on the logs configuration page before deleting.

PAM-CMN-1981 = Session recording purging already running

PAM-CMN-1982 = Session recording purging started...

PAM-CMN-1983 = File storage went down while session recording purging was in progress

PAM-CMN-1984 = Session recording purging successfully completed. {0} recording(s) was/were removed. Took {1} seconds

PAM-CMN-1985 = Starting session reconciliation run.

PAM-CMN-1986 = Session recording reconciliation process still running. This may indicate a problem with your system; please contact Broadcom Support if you see this message occurring frequently.

PAM-CMN-1987 = Unable to delete short file {0}

PAM-CMN-1988 = Deleted short file {0}

PAM-CMN-1989 = Ending session recording reconciliation. {0} session recording rows added to table. {1} sidecar(.inf) files added to share. {2} nearly empty files deleted from share.

PAM-CMN-1990 = Unable to mount NFS after 2 attempts

PAM-CMN-1991 = Unable to mount SMB after 2 attempts

PAM-CMN-1992 = Unable to mount Amazon S3 bucket after 2 attempts

PAM-CMN-1993 = rfscheck[{0}]: "Unable to mount NFS after 2 attempts"

PAM-CMN-1994 = rfscheck[{0}]: "Unable to mount SMB after 2 attempts"

PAM-CMN-1995 = rfscheck[{0}]: "Unable to mount Amazon S3 bucket after 2 attempts"

PAM-CMN-2121 = Session recording mitigation not applied because API user lacked the privilege

PAM-CMN-2122 = Session recording mitigation not applied. No privilege manager in session.

PAM-CMN-2199 = Updated filters and session recording

PAM-CMN-2207 = Session Recording

PAM-CMN-2209 = CLI Session Recording: on;

PAM-CMN-2210 = CLI Session Recording: off;

PAM-CMN-2211 = Graphical Session Recording: on;

PAM-CMN-2212 = Graphical Session Recording: off;

PAM-CMN-2213 = Web Session Recording: on;

PAM-CMN-2214 = Web Session Recording: off;

PAM-CMN-2218 = CLI Session Recording: on bidirectional;  
 PAM-CMN-2219 = CLI Session Recording: off bidirectional;  
 PAM-CMN-2403 = Session recording started for {0}. {1}  
 PAM-CMN-2404 = Session recording stopped for {0}. {1}  
 PAM-CMN-2503 = Reported problem on NFS for Session Recording  
 PAM-CMN-2505 = Reported problem with NFS share for Session Recording  
 PAM-CMN-2507 = Reported problem on Amazon S3 for Session Recording  
 PAM-CMN-2509 = Reported problem on SMB for Session Recording  
 PAM-CMN-2728 = Storage is not mounted, can not start session recording.  
 PAM-CMN-2730 = gatekeeper[{0}]: Fail to initialize recoding, security safe mode, service discarded  
 PAM-CMN-2804 = Session can't be established due to a problem with session recording  
 PAM-CMN-3134 = Primary network storage for session recording is down  
 PAM-CMN-3220 = Failed to enable session recording on the fly, security safe mode  
 PAM-CMN-3224 = There was a problem with the recording storage. This connection is not allowed in security-safe mode.  
 PAM-CMN-3333 = Current session recording file "{0}" is broken or refers to other CA PAM.  
 PAM-CMN-3334 = Access Denied!  
 PAM-CMN-3354 = There is insufficient space to play the recording at this time. Please try again later.  
 PAM-CMN-3355 = Invalid host id specified.

## Session Manager Service Messages

PAM-CMN-1341 = This CA PAM appliance is in maintenance mode. Only admin users will be able to login.  
 PAM-CMN-4100 = Session log records must be in an array.  
 PAM-CMN-4101 = Session log record {0} is invalid.  
 PAM-CMN-4102 = Ignore session log level flag {0} is invalid. Value should be 1 for true, 0 for false.  
 PAM-CMN-4103 = Session log transaction type {0} is invalid. See documentation for a list of valid types.  
 PAM-CMN-4014 = Created timestamp {0} is invalid. It should be number of milliseconds since the epoch or empty.

## Upgrade, Backup, and Recovery Messages

PAM-CMN-1342 = Applied patch '{0}'. {1}  
 PAM-CMN-1343 = Upgrading to the same version could cause unexpected result  
 PAM-CMN-1344 = Problem applying the upgrade package. Details: {0}  
 PAM-CMN-1345 = Please stop the cluster before proceeding with the upgrade  
 PAM-CMN-1346 = Upgrade package has been applied successfully  
 PAM-CMN-1347 = Backup of the appliance takes time. Please be patient and wait until it reboots.<br/>The LCD will show the message <b>System backup! Please wait!</b> <br/> Wait until the normal operation message shows on the LCD then log in again and resume work in your browser.  
 PAM-CMN-1348 = Recover of the appliance takes time. Please be patient and wait until it reboots.<br/>The LCD will show the message <b>System backup! Please wait!</b><br/> Wait until the normal operation message shows on the LCD then log in again and resume work in your browser.  
 PAM-CMN-1349 = An error occurred while running the backup  
 PAM-CMN-1350 = An error occurred while running recovery  
 PAM-CMN-1351 = Configuration-Upgrade: Performing Backup

PAM-CMN-1352 = Configuration-Recovery: Performing Recovery

PAM-CMN-1353 = An error occurred while trying to delete the staging file

PAM-CMN-3278 = FAILED TO RESTORE DB. {0} is too big to restore the database safely!

PAM-CMN-3279 = DB can be restored successfully. Required DB size is less than Existing DB

PAM-CMN-3280 = FAILED TO RESTORE DB. {0} is too big to restore. Required SPACE={1} kb

PAM-CMN-3281 = DB can be successfully restored. Required Disk space={0}, HALF of Available Space={1}

PAM-CMN-3282 = {0} is not a writable directory.

PAM-CMN-3283 = A fatal error occurred while dumping the database.

PAM-CMN-3284 = Database dumped successfully to {0}

PAM-CMN-3285 = The database you are attempting to load is not compatible with the current version.

PAM-CMN-3286 = This database contains settings that are not compatible with FIPS mode. Turn off FIPS mode to continue restoring.

PAM-CMN-3287 = An error occurred while trying to load {0}.

PAM-CMN-3288 = Allows the use of the External API by {0}.

PAM-CMN-3335 = Cannot access patchinfo file. This patch must be an older package type, not installable on this version of CA PAM.

PAM-CMN-3336 = CA PAM cannot be upgraded while in cluster mode. Turn off clustering before upgrading.

PAM-CMN-3337 = Insufficient storage space for successful firmware upgrade.<br>Export your logs to free storage space and try again.

PAM-CMN-3338 = Problem unpacking the upgrade package.

PAM-CMN-3339 = This is an invalid FIPS patch. Please contact Broadcom Support.

PAM-CMN-3340 = Patch verification failed.

PAM-CMN-3341 = This is not an approved FIPS patch.

PAM-CMN-3342 = Insufficient storage for database update.<br>Export your logs and try to upgrade again.

PAM-CMN-3343 = Unable to check the upgrade package version.<br>The package seems to be older. CA PAM cannot be downgraded.

PAM-CMN-3344 = Cannot upgrade CA PAM.

PAM-CMN-3345 = Cannot upgrade because current<br>CA PAM version {0} must equal {1}.

PAM-CMN-3346 = Cannot upgrade because current<br>CA PAM version {0} must be between {2} and {3} (inclusive).

PAM-CMN-3347 = Could not export record of type "{0}" initiated by user "{1}". Error message: "{2}".

PAM-CMN-3349 = Cannot upgrade because patch is not HMAC signed. Please contact Broadcom Support.

PAM-CMN-3350 = Cannot upgrade because patch has invalid checksum. Please contact Broadcom Support.

PAM-CMN-3367 = Cannot upgrade because {0} cannot be installed on CA PAM {1}. <br>To upgrade from CA PAM {2}, please use CA PAM {3}. {4} once available.

PAM-CMN-3382 = The last full appliance backup failed on {0}

## CA Threat Analytics Related Messages

PAM-CMN-1028 = CA Threat Analytics server is inaccessible or its configuration is invalid.

PAM-CMN-1354 = CA Threat Analytics update failed. Message (if any) was {0}

PAM-CMN-1355 = CA Threat Analytics update succeeded in part and failed in part.

PAM-CMN-1356 = CA Threat Analytics get failed.

PAM-CMN-1357 = CA Privileged Access Manager is collecting and analyzing limited information about your client system and sessions

PAM-CMN-2032 = BAPService.getRiskLevels called when {0} was not configured. Request ignored.

PAM-CMN-2033 = BAPService.getUserRiskLevels called when {0} was not configured. Request ignored.

PAM-CMN-2034 = User Id {0} invalid for BAPService.getUserRiskLevel.



PAM-CMN-2035 = User {0} was assigned a risk level from {1}.

PAM-CMN-2036 = User {0} was assigned the default risk level.

PAM-CMN-2037 = Session id was not in proper format. Data was not sent to {0}.

PAM-CMN-2038 = Unexpected action {0} while trying to log a connect or disconnect. Expected values are connect or disconnect

PAM-CMN-2039 = Invalid connection id {0} when attempting to log a {1} event.

PAM-CMN-2040 = No connection found with sequence number {0}. {1} was not logged to {2}.

PAM-CMN-2041 = Unexpected reason {0} for disconnecting from client. Disconnection will not be logged.

PAM-CMN-2042 = Default risk level not found. A risk level of Good will be used.

PAM-CMN-2043 = Unexpected default risk level {0}. A risk level of Good will be used.

PAM-CMN-2044 = Missing required service identifier. Data was not reported to {0}.

PAM-CMN-2045 = Invalid url {0} for sending to {1}.

PAM-CMN-2046 = Unable to construct {0} URL. Message was {1}

PAM-CMN-2047 = extraData should be an array or empty

PAM-CMN-2048 = Warning: extra parameters supplied will be ignored because the url contains a query string

PAM-CMN-2049 = Invalid request type {0} - one of GET, POST, PUT, or DELETE should be used

PAM-CMN-2050 = Unable to find {0} Authorization token. Message was {1}.

PAM-CMN-2051 = Invalid administrative user id {0} when attempting to log a session logout

PAM-CMN-2052 = Invalid logout reason {0} when attempting to log a session logout

PAM-CMN-2053 = Session id was not in proper format. Data was not sent to {0}.

PAM-CMN-2054 = Unable to get user information for logout based on administrator userid: {0}.

PAM-CMN-2055 = Private IP address was not in proper format. Data was not sent to {0}.

PAM-CMN-2056 = Public IP address was not in proper format. Data was not sent to {0}.

PAM-CMN-2057 = Machine id was not in proper format. Data was not sent to {0}.

PAM-CMN-2058 = No session found for session {0} uplnit data will not be sent to {1}.

PAM-CMN-2790 = User must have configuration manager, manage devices and manage network services privileges to update the TAP configuration

PAM-CMN-2791 = Invalid address {0} supplied for TAP device. Update failed.

PAM-CMN-3615 = Created {0} Admin Group with group name {1}.

PAM-CMN-3616 = {0} group already exists, was not changed.

PAM-CMN-3617 = Threat Analytics special user group is deleted when Threat Analytics is no longer licensed, and may not be deleted otherwise.

PAM-CMN-3618 = Deleted {0} Admin Group {1}.

PAM-CMN-3619 = Threat Analytics special user group cannot be updated.

PAM-CMN-3621 = Threat Analytics special policy cannot be deleted.

PAM-CMN-3622 = Threat Analytics special policy cannot be updated.

PAM-CMN-3623 = Threat Analytics special user group should have super user as one of its members.

PAM-CMN-3624 = Only Users with Global Administrator privilege can be added to Threat Analytics special user group and vice versa.

## Active Directory Messages

PAM-CMN-2177 = The user must reset their password.

PAM-CMN-2178 = The user's password has expired.

PAM-CMN-2179 = The user entered an incorrect password.

PAM-CMN-2180 = The user's account is disabled in Active Directory.

PAM-CMN-2181 = The user's account has expired in Active Directory.

PAM-CMN-2182 = The user's account has been locked in Active Directory.

PAM-CMN-2183 = The user's account cannot be found in Active Directory.

PAM-CMN-2184 = The user is not permitted to login in Active Directory.

PAM-CMN-2185 = The user is not permitted to login on this workstation in Active Directory.

## SAML Related Messages

PAM-CMN-1360 = PAM received a request to issue an assertion for SAML service {0}, but the user is not authorized to access this service.

PAM-CMN-1361 = SAML assertion for service {0} will not be released because the subject name ID format was not specified in the policy for this user.

PAM-CMN-1362 = SAML assertion for service {0} will not be released because the following required attributes have not been mapped or resolved to a value: {1}

PAM-CMN-1363 = PAM SAML IdP issued an authentication failed response to SAML service {0} with entity ID {1} via {2}

PAM-CMN-1364 = PAM SAML IdP issued an authentication failed response to SAML service {0} with entity ID {1} via {2} authenticated via {3}

PAM-CMN-1365 = PAM SAML IdP has issued an assertion to SAML service {0} with entity ID {1} via {2} as subject {3}

PAM-CMN-1366 = PAM SAML IdP has issued an assertion to SAML service {0} with entity ID {1} via {2} as subject {3} authenticated via {4}

PAM-CMN-1367 = There is a SAML Subject Identifier Format policy conflict for user {0} for SAML service {1} involving the following policies: {2}

PAM-CMN-1368 = There is a SAML Subject Identifier Value policy conflict for user {0} for SAML service {1} involving the following policies: {2}

PAM-CMN-1369 = PAM SAML IdP request: Message did not meet security requirements. {0}

PAM-CMN-1370 = PAM received a request to issue an assertion for recorded SAML service {0}, but the user did not access the service using the PAM browser, as required for web session recording. The user must access the service using the PAM browser from the PAM Access page.

PAM-CMN-1520 = PAM SAML IdP request: {0}

PAM-CMN-1731 = SAML SSO Enabled

PAM-CMN-1732 = SAML SSO Disabled

PAM-CMN-1908 = PAM SAML IdP request: Message did not meet security requirements. Authentication request received from unknown SAML SP {0}

PAM-CMN-2158 = Error parsing the SAML metadata file.

PAM-CMN-2159 = Metadata file does not contain any SAML IdP entities.

PAM-CMN-2160 = SAML entity {0} does not contain a SingleSignOnService with a valid Post binding. Acceptable Post bindings are: {1}.

PAM-CMN-2161 = SAML entity {0} does not contain a SingleSignOnService with a Post or Redirect binding.

PAM-CMN-2162 = SAML entity {0} does not contain any key data.

PAM-CMN-2163 = There are no valid SAML 2.0 IdP descriptors in the metadata file.

PAM-CMN-2164 = SAML Remote IdP(s) added: {0}.

PAM-CMN-2186 = SAML user provisioned via Just In Time provisioning from Remote Identity Provider {0}

PAM-CMN-2747 = SAML configuration (except Fully Qualified Hostname) will be replicated to all cluster members

PAM-CMN-5388 = Refreshing the metadata for SAML identity provider %s failed. Please ensure the source URL is accessible and that if configured for validation, that the certificate fingerprint corresponds to the certificate used to sign the metadata.

PAM-CMN-5389 = Metadata refresh is enabled but there are no IdPs configured with a source URL for metadata refresh.

PAM-CMN-5390 = SAML metadata refresh for IdP %s completed successfully but there were no updates.

PAM-CMN-5391 = SAML metadata refresh for IdP %s completed successfully: %s certificates added, %s certificates removed.

PAM-CMN-5392 = Saving the updated certificates during SAML metadata refresh failed with the following error: %s

PAM-CMN-5393 = Specifying the fingerprint for the metadata refresh signing certificate requires the source URL where the metadata can be retrieved.

PAM-CMN-5394 = The metadata source URL is not a valid URL.

PAM-CMN-5395 = Specified metadata refresh certificate fingerprint is not a valid SHA-1 certificate fingerprint.

PAM-CMN-5396 = Invalid SP metadata refresh mode specified.

## SSL, FIPS, and Cryptography Messages

PAM-CMN-2724 = OpenSSL configuration error: {0}, {1}

PAM-CMN-2831 = PAM is currently provisioned to use OpenSSL and the password is not cached!  
PAM-CMN-2832 = PAM is re-encrypting the DB. Please try again later.

PAM-CMN-2837 = PAM is currently provisioned to use WolfSSL and the password is not cached!

PAM-CMN-2848 = Proper usage: useOpenSSL <provider>

PAM-CMN-2849 = password and confirmed password do not match!

PAM-CMN-2851 = PAM is currently provisioned to use non-FIPS mode cryptography provider

PAM-CMN-2852 = PAM is currently provisioned to use FIPS mode cryptography provider

PAM-CMN-3105 = Warning: client selects unsupported cipher.

PAM-CMN-3107 = WolfSSL JNI library result: {0}, Replicating WolfSSL config settings to non primary members

PAM-CMN-3108 = WolfSSL JNI library result: {0}, Memory allocation error in getKeyFromLabel

PAM-CMN-3109 = WolfSSL JNI library result: {0}, failed to decrypt the key in getKeyFromLabel

PAM-CMN-3110 = WolfSSL JNI library result: {0}, Failed to logon to WolfSSL JNI layer

PAM-CMN-3111 = WolfSSL JNI library result: {0}, Failed to generate random AES key with RDRAND

PAM-CMN-3112 = WolfSSL JNI library result: {0}, Failed to generate random AES key using WolfSSL

PAM-CMN-3113 = WolfSSL JNI library result: {0}, Successfully generated the random AES key with WolfSSL

PAM-CMN-3114 = WolfSSL JNI library result: {0}, Failed to encrypt the secret key

PAM-CMN-3115 = WolfSSL JNI library result: {0}, Failed to PEM encode the secret key

PAM-CMN-3116 = WolfSSL JNI library result: {0}, Failed to find label to encrypt

PAM-CMN-3117 = WolfSSL JNI library result: {0}, Failed to get key to encrypt

PAM-CMN-3118 = WolfSSL JNI library result: {0}, Failed to get input string to encrypt

PAM-CMN-3119 = WolfSSL JNI library result: {0}, Failed to encrypt since input string is zero length

PAM-CMN-3120 = WolfSSL JNI library result: {0}, Encryption failed. The result is empty

PAM-CMN-3121 = WolfSSL JNI library result: {0}, Failed to find label to decrypt

PAM-CMN-3122 = WolfSSL JNI library result: {0}, Failed to get key to decrypt

PAM-CMN-3123 = WolfSSL JNI library result: {0}, Failed to get input string to decrypt

PAM-CMN-3124 = WolfSSL JNI library result: {0}, Failed to decrypt since input string is zero length  
PAM-CMN-3125 = WolfSSL JNI library result: {0}, Decryption failed. The result is empty  
PAM-CMN-3165 = WolfSSL JNI library result: {0}, Successfully generated the random AES key with hardware RDRAND  
PAM-CMN-3166 = SSL Config result: {0}, Failed to generate random data using hardware RDRAND  
PAM-CMN-3167 = SSL Config result: {0}, Failed to generate random data using OpenSSL  
PAM-CMN-3168 = SSL Config result: {0}, Failed to open masking file for writing  
PAM-CMN-3173 = SSL Config result: {0}, Encryption test error!  
PAM-CMN-3174 = SSL Config result: {0}, Failed to open encryption test file for writing  
PAM-CMN-3175 = SSL Config result: {0}, Memory allocation error  
PAM-CMN-3176 = SSL Config result: {0}, Failed to PEM encode the masked password  
PAM-CMN-3177 = SSL Config result: {0}, Failed to open password file for writing  
PAM-CMN-3178 = SSL Config result: {0}, Failed to open masking file for reading  
PAM-CMN-3180 = SSL Config result: {0}, Failed to open password file for reading  
PAM-CMN-3191 = SSL Config result: {0}, Successfully generated random data with hardware RDRAND  
PAM-CMN-3192 = SSL Config result: {0}, Successfully generated random data with OpenSSL  
PAM-CMN-3193 = SSL Config result: {0}, Failed to generate random data using WolfSSL  
PAM-CMN-3194 = SSL Config result: {0}, Successfully generated random data with WolfSSL  
PAM-CMN-3195 = SSL Config result: {0}, Failed to generate master passphrase using hardware RDRAND  
PAM-CMN-3196 = SSL Config result: {0}, Failed to generate master passphrase using OpenSSL  
PAM-CMN-3197 = SSL Config result: {0}, Successfully generated master passphrase with hardware RDRAND  
PAM-CMN-3198 = SSL Config result: {0}, Successfully generated master passphrase with OpenSSL  
PAM-CMN-3199 = SSL Config result: {0}, Failed to generate master passphrase using WolfSSL  
PAM-CMN-3200 = SSL Config result: {0}, Successfully generated master passphrase with WolfSSL  
PAM-CMN-3294 = OpenSSL JNI library result: {0}, No cached OpenSSL password, using default key  
PAM-CMN-3295 = OpenSSL JNI library result: {0}, Replicating OpenSSL config settings to non primary members  
PAM-CMN-3296 = OpenSSL JNI library result: {0}, Memory allocation error in getKeyFromLabel  
PAM-CMN-3297 = OpenSSL JNI library result: {0}, ERROR, Non default OpenSSL key and OpenSSL password is not cached.  
PAM-CMN-3298 = OpenSSL JNI library result: {0}, Memory allocation error in getKeyFromLabel  
PAM-CMN-3299 = OpenSSL JNI library result: {0}, failed to decrypt the key in getKeyFromLabel  
PAM-CMN-3302 = OpenSSL JNI library result: {0}, Successfully generated the random AES key with hardware RDRAND  
PAM-CMN-3303 = OpenSSL JNI library result: {0}, Failed to generate random AES key using OpenSSL  
PAM-CMN-3304 = OpenSSL JNI library result: {0}, Successfully generated the random AES key with OpenSSL  
PAM-CMN-3305 = OpenSSL JNI library result: {0}, Failed to logon to OpenSSL JNI layer, using defaults  
PAM-CMN-3306 = OpenSSL JNI library result: {0}, Failed to generate random AES key with hardware RDRAND  
PAM-CMN-3307 = OpenSSL JNI library result: {0}, Failed to encrypt the secret key  
PAM-CMN-3308 = OpenSSL JNI library result: {0}, Failed to PEM encode the secret key  
PAM-CMN-3309 = OpenSSL JNI library result: {0}, Failed to find label to encrypt  
PAM-CMN-3310 = OpenSSL JNI library result: {0}, Failed to get key to encrypt  
PAM-CMN-3311 = OpenSSL JNI library result: {0}, Failed to get input string to encrypt  
PAM-CMN-3312 = OpenSSL JNI library result: {0}, Failed to encrypt since input string is zero length  
PAM-CMN-3313 = OpenSSL JNI library result: {0}, Encryption failed. The result is empty  
PAM-CMN-3314 = OpenSSL JNI library result: {0}, Failed to find label to decrypt  
PAM-CMN-3315 = OpenSSL JNI library result: {0}, Failed to get key to decrypt  
PAM-CMN-3316 = OpenSSL JNI library result: {0}, Failed to get input string to decrypt  
PAM-CMN-3317 = OpenSSL JNI library result: {0}, Failed to decrypt since input string is zero length  
PAM-CMN-3318 = OpenSSL JNI library result: {0}, Decryption failed. The result is empty

## Other Common Messages

PAM-CMN-1359 = CA Single Sign-On disabled. Rebooting Apache...

PAM-CMN-1371 = Log records viewed

### NOTE

The PAM-CMN-1371 message appears twice when someone logs into the CA PAM UI. This is expected behavior as the UI queries the log to obtain information to appear under **Recent Events** and to populate the dashboard.

PAM-CMN-1372 = Downloaded log records

PAM-CMN-1373 = Failed to update status of log row {0}

PAM-CMN-1374 = Log report {0} successfully added

PAM-CMN-1375 = Log report {0} not added

PAM-CMN-1376 = Log report {0} updated

PAM-CMN-1377 = Update of log report {0} failed

PAM-CMN-1378 = Log report {0} was deleted

PAM-CMN-1379 = Log report {0} was not deleted

PAM-CMN-1380 = Unable to retrieve all device data for applet. Check device properties and terminal types for device.

PAM-CMN-1381 = Credential service is down, user must enter their own credentials

PAM-CMN-1382 = Credential not found for association

PAM-CMN-1383 = Missing session host data for device, unable to launch applet

PAM-CMN-1386 = Unable to find sequence number for device {0} service {1} protocol {2}

PAM-CMN-1387 = Check Conflicts require either a task or a service to check against.

PAM-CMN-1389 = Unable to find secondary login credential for transparent login

PAM-CMN-1390 = CSV {0} of type {1} initiated by user {2}.

PAM-CMN-1391 = CSV {0} of type {1} initiated by user {2} completed in {3}.

PAM-CMN-1392 = A CSV import/export job is already running and is at {0} percent completion. Please wait until it is complete before initiating another.

PAM-CMN-1393 = A CSV {0} of {1} is running in the background and is at {2} percent completion. It has been running for {3}.

PAM-CMN-1394 = A CSV {0} of {1} is running in the background and is at {2} percent completion. It has been running for {3}. Please wait until it is complete before initiating another.

PAM-CMN-1395 = Downloaded CSV output file {0} generated from the {1} of {2}.

PAM-CMN-1396 = Error running scheduled database backup - unable to retrieve account information.

PAM-CMN-1397 = Error running scheduled database backup - Invalid number of parameters.

PAM-CMN-1398 = Credential service is down

PAM-CMN-1399 = Error obtaining device information for backup destination

PAM-CMN-1400 = Error obtaining target IP for backup destination

PAM-CMN-1401 = Invalid device address {0}. Address should be IP address or hostname.

PAM-CMN-1402 = An error occurred while uploading patch. Unknown error

PAM-CMN-1403 = An error occurred while uploading patch. File is not uploaded

PAM-CMN-1404 = An error occurred while uploading patch. Can't move file to staging folder

PAM-CMN-1405 = An error occurred while uploading patch. No file was uploaded

PAM-CMN-1406 = An error occurred while uploading patch. Invalid file size

PAM-CMN-1407 = An error occurred while uploading patch. File was uploaded partially

PAM-CMN-1408 = Unauthorized access to Upgrade service

PAM-CMN-1409 = Patch with name: {0} already exists

PAM-CMN-1410 = Ready to apply patch: {0}. Reboot required

PAM-CMN-1411 = This upgrade requires a reboot of the system.

PAM-CMN-1412 = Incorrect file name {0}. Patch not found.

PAM-CMN-1413 = Error in canceling apply patch process.

PAM-CMN-1414 = Wrong file type, please select again.



PAM-CMN-1415 = Patch with name '{0}' has been uploaded successfully.

PAM-CMN-1416 = Specified patch file does not exist.

PAM-CMN-1417 = PAM appliance ({0}) attempted to perform cluster operation, but is not part of the cluster list.

PAM-CMN-1418 = Error retrieving credential id. Message was {0}

PAM-CMN-1419 = The credential with the id {0} is not used in any policy for this user and device {1}.

PAM-CMN-1420 = Target account: {0}

PAM-CMN-1421 = User {0}'s access to applet(s) {1} and service(s) {2} on device {3} disabled due to policy conflicts. Navigate to the View Conflicts page for more details.

PAM-CMN-1422 = User {0}'s access to applet(s) {1} on device {2} disabled due to policy conflicts. Navigate to the View Conflicts page for more details.

PAM-CMN-1423 = User {0}'s access to service(s) {1} on device {2} disabled due to policy conflicts. Navigate to the View Conflicts page for more details.

PAM-CMN-1424 = User {0}'s connection to {1} has multiple command filter {2} list policies. Enforcing union of command filter policies: {3}.

PAM-CMN-1425 = User '{0}' attempted to access the unauthorized page: {1}.

PAM-CMN-1426 = Ping test: Error connecting to {0}.

PAM-CMN-1427 = setServletState: Error connecting to the Server Control integration servlet.

PAM-CMN-1428 = getEncryptedPassword: Could not encrypt the password. res={0}

PAM-CMN-1429 = An error occurred clearing Server Control integration data.

PAM-CMN-1430 = Failed to insert into configuration table (name = '{0}', value = '{1}')

PAM-CMN-1431 = Failed to update configuration table (name = '{0}', value = '{1}')

PAM-CMN-1432 = An error occurred saving Server Control integration data.

PAM-CMN-1433 = An error occurred contacting Server Control integration servlet.

PAM-CMN-1434 = Deleted certificate: {0}

PAM-CMN-1435 = User switched to Configuration Section

PAM-CMN-1436 = Unauthorized connection to /config2/ from IP {0}.

PAM-CMN-1437 = PAM Config Login OK.

PAM-CMN-1449 = Updates in Global Settings: {0}

PAM-CMN-1450 = Invalid limit specified for query. Value was {0}. Limit was ignored.

PAM-CMN-1451 = Invalid offset specified for query. Value was {0}. Offset was ignored.

PAM-CMN-1452 = Downloaded database backup public key file {0}.

PAM-CMN-1453 = Error downloading database backup public key file.

PAM-CMN-1454 = S3 mount operation unsuccessful. {0}.

PAM-CMN-1455 = S3 bucket already mounted. {0}.

PAM-CMN-1457 = Created System Diagnostic file

PAM-CMN-1458 = Remote PAM Debugging Services turned {0}

PAM-CMN-1459 = External logging failure

PAM-CMN-1468 = User session initialized ({0})

PAM-CMN-1469 = User switched to Administration Section

PAM-CMN-1470 = User {0} attempted to access the unauthorized feature: {1}.

PAM-CMN-1471 = Importing {0} from file {1} aborted. Imported: {2}, Added: {3}, Updated: {4}, Errors: {5}. {6}/{7} {0} imported before abort.

PAM-CMN-1472 = Imported {0} from file {1}. Imported: {2}, Added: {3}, Updated: {4}, Errors: {5}.

PAM-CMN-1473 = Super username changed from ({0}) to ({1}).

PAM-CMN-1474 = PAM denied unauthorized JAR download request to {0}.

PAM-CMN-1475 = JAR file {0} was not found.

PAM-CMN-1476 = Invalid LDAP domain specified for authenticating user {0}.

PAM-CMN-1477 = Unable to retrieve LDAP servers for domain {0} for authenticating user {1}.

PAM-CMN-1478 = Unauthorized connection to /config/ from IP {0}.

PAM-CMN-1479 = Uploaded license file "{0}".

PAM-CMN-1480 = {0} {1} copied from {2}. Copied all {3} associations!

PAM-CMN-1481 = Session expired

PAM-CMN-1482 = Logout OK  
PAM-CMN-1483 = Office 365 policy between user {0} and device {1} deleted.  
PAM-CMN-1484 = Association between user {0} and device {1} deleted.  
PAM-CMN-1485 = Association between user {0} and device {1} does not contain any services, SSL VPN services, or applets. Removing association.  
PAM-CMN-1486 = The CA PAM database has been reset successfully.  
PAM-CMN-1487 = Database backup schedule deleted successfully!  
PAM-CMN-1488 = Problem deleting the database backup schedule!  
PAM-CMN-1489 = Unable to save the database backup schedule!  
PAM-CMN-1505 = Did not add virtual device {0} to the non-existent group {1}  
PAM-CMN-1506 = Did not add virtual device {0} to the non-AWS group {1}  
PAM-CMN-1510 = Unauthorized attempt to retrieve device groups by {0}  
PAM-CMN-1511 = Unauthorized attempt to add a device group by {0}  
PAM-CMN-1512 = Unauthorized attempt to update device group by user {0}  
PAM-CMN-1513 = Unauthorized attempt to update properties of device group {0} by {1}.  
PAM-CMN-1514 = Unauthorized attempt to add devices to group {0} by {1}.  
PAM-CMN-1515 = Unauthorized attempt to delete a device group by {0}  
PAM-CMN-1516 = Device Group {0} successfully deleted  
PAM-CMN-1517 = Device Group {0} was not found and not deleted  
PAM-CMN-1518 = Unexpected result from deleting device group  
PAM-CMN-1519 = Unauthorized attempt to delete device group {0} by {1}  
  
PAM-CMN-1521 = {0} device group(s) deleted, {1} device group(s) not deleted for lack of privilege, {2} device group(s) not found, {3} unknown device group delete errors.  
PAM-CMN-1522 = Special type device {0} deleted  
PAM-CMN-1523 = Special type device {0} not deleted  
PAM-CMN-1524 = Special type device {0} updated  
PAM-CMN-1525 = Special type device {0} not updated  
PAM-CMN-1526 = User Defined Special type device {0} inserted  
PAM-CMN-1527 = Special type device {0} not inserted  
PAM-CMN-1528 = Database corruption - more than one special type device was inserted  
PAM-CMN-1529 = User {0} tried to update device  
PAM-CMN-1530 = Unauthorized attempt to update device {0} by {1}  
PAM-CMN-1531 = Unknown expected response from multi device delete. Response = {0} for device id {1}  
PAM-CMN-1532 = Completely unexpected response {0} when deleting device  
PAM-CMN-1533 = Device was not found and not deleted - disregard message above  
PAM-CMN-1534 = Device {0} was not found and not deleted - disregard delete log message above  
PAM-CMN-1535 = Unexpected result from deleting device  
PAM-CMN-1536 = Unauthorized attempt to add a device {0} by {1}  
PAM-CMN-1537 = User {0} tried to autoregister device {1} without authorization  
PAM-CMN-1538 = User {0} tried to change the host name of a device via autoregistration without authorization  
PAM-CMN-1539 = Device {0} is not a request server, but has a request server id. The address was not updated.  
PAM-CMN-1540 = User {0} tried to update the target server without proper privileges without authorization  
PAM-CMN-1541 = User {0} not authorized to delete device  
PAM-CMN-1542 = User {0} tried to assign device {1} to device groups {2} without authorization  
PAM-CMN-1543 = User {0} tried to {1} device {2} without assigning the device to an authorized group.  
PAM-CMN-1544 = Unexpected provisioning type id when updating {0}  
PAM-CMN-1545 = User {0} tried to initiate autodiscovery without authorization  
PAM-CMN-1546 = Mismatch on provision types in reconcile virtual devices. Expected {0} got {1}  
PAM-CMN-1548 = Unknown response when adding ldap group {0}  
PAM-CMN-1549 = Session recording purging settings updated.  
PAM-CMN-1551 = Unauthorized attempt to update smart button group {0} by {1}  
PAM-CMN-1552 = Unauthorized attempt to add smart button group {0} by user {1}

PAM-CMN-1553 = Smart Button group {0} added.  
PAM-CMN-1554 = Smart Button group {0} not added  
PAM-CMN-1555 = Database corruption - more than one Smart Button group was added  
PAM-CMN-1556 = Unauthorized attempt to delete smart button group {0} by {1}  
PAM-CMN-1557 = Successfully deleted smart button group {0}  
PAM-CMN-1558 = Smart Button group {0} was not found and not deleted  
PAM-CMN-1559 = Unexpected result from deleting smart button group  
PAM-CMN-1560 = Unauthorized attempt to access group list by {0}  
PAM-CMN-1561 = Tag {0} was renamed to {1}  
PAM-CMN-1562 = Tag {0} was deleted  
PAM-CMN-1563 = User {0} tried to manage tags without authorization  
PAM-CMN-1564 = User {0} tried to rename a label to {1} without authorization  
PAM-CMN-1565 = User {0} tried to delete a label without authorization  
PAM-CMN-1566 = Unauthorized attempt to change user group {0} by {1}  
PAM-CMN-1567 = User group {0} successfully updated  
PAM-CMN-1568 = Database corruption - more than one user group was updated  
PAM-CMN-1569 = Unauthorized attempt to add users to groups by {0}  
PAM-CMN-1570 = Unauthorized attempt to add users to group {0} by {1}  
PAM-CMN-1571 = Unauthorized attempt to add user group {0} by {1}  
PAM-CMN-1572 = User group {0} not inserted  
PAM-CMN-1573 = Database corruption - more than one user group was inserted  
PAM-CMN-1574 = {0} user group(s) deleted, {1} user group(s) not deleted for lack of privilege, {2} user group(s) not found, {3} unknown user group delete errors  
PAM-CMN-1575 = Unauthorized attempt to delete user group {0} by {1}  
PAM-CMN-1576 = User group {0} successfully deleted  
PAM-CMN-1577 = User group {0} was not found and not deleted  
PAM-CMN-1578 = Unexpected result from deleting user group  
PAM-CMN-1579 = Unauthorized attempt to get user groups by {0}  
PAM-CMN-1580 = Unauthorized attempt to access group id {0} by {1}  
PAM-CMN-1581 = Unauthorized attempt to access group name {0} by {1}  
PAM-CMN-1582 = User {0} not found or not authorized to read, so it was not deleted  
PAM-CMN-1583 = {0} user(s) deleted, {1} user(s) not deleted for lack of privilege, {2} user(s) not found, {3} ldap users not deleted, {4} login contact user(s) not deleted, {5} unknown user delete errors  
PAM-CMN-1584 = User {0} tried to add user {1} without authorization  
PAM-CMN-1585 = User {0} did not have name set, so it was not updated  
PAM-CMN-1586 = User {0} tried to update user {1} without authorization  
PAM-CMN-1587 = Unauthorized Attempt to update user {0} with id {1}. This method can only update the logged in user.  
PAM-CMN-1588 = Unauthorized attempt to change user fields on self update  
PAM-CMN-1589 = User {0} not deleted or another user deleted them  
PAM-CMN-1590 = User {0} tried to retrieve the list of smart button groups without authorization  
PAM-CMN-1599 = User {0} tried to add target server {1} without authorization  
PAM-CMN-1600 = User {0} tried to delete PA user {1} without authorization  
PAM-CMN-1601 = No PM user groups found for a user with credential manager privilege  
PAM-CMN-1602 = User {0} tried to update target server {1} without authorization  
PAM-CMN-1603 = Target server {0} unexpectedly not found  
PAM-CMN-1604 = Target server {0} updated and renamed to {1}  
PAM-CMN-1605 = Request server {0} unexpectedly not found.  
PAM-CMN-1606 = User {0} tried to delete target server {1} without authorization  
PAM-CMN-1607 = User {0} tried to add request server {1} without authorization  
PAM-CMN-1608 = User {0} tried to delete request server {1} without authorization  
PAM-CMN-1609 = User {0} tried to add service {1} without authorization  
PAM-CMN-1610 = Failed to add service {0}.  
PAM-CMN-1611 = Database corruption - more than one service was inserted



PAM-CMN-1612 = Service {0} not added  
PAM-CMN-1613 = User {0} tried to add SSL VPN service {1} without authorization  
PAM-CMN-1614 = SSL VPN Service {0} not added.  
PAM-CMN-1615 = Database corruption - more than one SSL VPN Service was inserted  
PAM-CMN-1616 = User {0} tried to update service {1} without authorization  
PAM-CMN-1617 = User {0} tried to update SSL VPN service {1} without authorization  
PAM-CMN-1618 = User {0} tried to delete service {1} without authorization  
PAM-CMN-1619 = Service {0} deleted  
PAM-CMN-1620 = User {0} tried to delete SSL VPN service {1} without authorization  
PAM-CMN-1621 = SSL VPN Service {0} deleted  
PAM-CMN-1622 = SSL VPN Service {0} not deleted  
PAM-CMN-1623 = Database corruption - more than one SSL VPN Service was deleted  
PAM-CMN-1624 = User {0} tried to retrieve services without authorization  
PAM-CMN-1625 = User {0} tried to retrieve SSL VPN service {1} without authorization  
PAM-CMN-1626 = User {0} tried to retrieve service {1} without authorization  
PAM-CMN-1627 = Unauthorized attempt to get role name list by {0}  
PAM-CMN-1628 = Unauthorized attempt to get role privileges by {0}  
PAM-CMN-1629 = Unauthorized attempt to update roles by {0}  
PAM-CMN-1630 = Attempt to update role {0} failed - no matching id  
PAM-CMN-1631 = Updated role {0}  
PAM-CMN-1632 = Unauthorized attempt to add role by {0}  
PAM-CMN-1633 = Attempt to create role {0} failed  
PAM-CMN-1634 = Role {0} has been created.  
PAM-CMN-1635 = Unauthorized attempt to delete role by {0}  
PAM-CMN-1636 = Attempted delete of role with a non-integer id {0}  
PAM-CMN-1637 = Attempt to change default role by {0}  
PAM-CMN-1638 = Deleted role {0}  
PAM-CMN-1639 = Unexpected result from deleting role - were multiple roles deleted?  
PAM-CMN-1640 = Unauthorized attempt to read roles by {0}  
PAM-CMN-1641 = Unauthorized attempt to read role details by {0}  
PAM-CMN-1642 = Unauthorized attempt to get restrictions for roles by {0}  
PAM-CMN-1643 = User {0}'s connection to {1} has multiple socket filter policies. Enforcing union of socket filter policies:  
{2}  
PAM-CMN-1644 = SSL VPN Configuration updated; Network: {0}/{1}  
PAM-CMN-1645 = SSL VPN Configuration updated; Network: {0}/{1}; Split tunneling enabled  
PAM-CMN-1648 = User attempted to connect via CA PAM Client but it is not permitted by configuration.  
  
PAM-CMN-1649 = Unable to retrieve the AWS Virtual Management IP provision region. The VIP cannot be managed on this node.  
PAM-CMN-1650 = Failed to initialize {0} user  
PAM-CMN-1651 = CA PAM Client connection terminated due to the empty Client Distribution URL  
PAM-CMN-1652 = There was an error retrieving credentials for AWS  
PAM-CMN-1653 = Unable to retrieve the AWS Virtual Management IP provision key. The VIP cannot be managed on this node.  
PAM-CMN-1654 = Attaching of additional storage to this virtual appliance ({0}) initiated, this appliance will be rebooted...  
PAM-CMN-1655 = Detaching of additional storage from this virtual appliance initiated, this appliance will be rebooted...  
PAM-CMN-1656 = Attachment of additional storage completed successfully  
PAM-CMN-1657 = Unable to retrieve AWS secret key for use by S3 storage.  
PAM-CMN-1658 = Detachment of additional storage completed successfully  
PAM-CMN-1659 = Invalid number of parameters sent to ldapDomainDelete. Nothing was deleted.  
PAM-CMN-1660 = Ldap domain {0} not found - delete aborted  
PAM-CMN-1661 = Run ping on host {0}  
PAM-CMN-1662 = Run traceroute on host {0}

PAM-CMN-1663 = Unable to traceroute {0}  
PAM-CMN-1664 = Failed to delete ldap servers from domain {0}. Domain will not be deleted.  
PAM-CMN-1665 = Failed to delete ldap domain {0}  
PAM-CMN-1666 = Scan Timeout! No results from the host! IP address: {0}. Ports: {1}  
PAM-CMN-1667 = Unable to scan the host! IP address: {0}. Ports: {1}  
PAM-CMN-1668 = The servers of LDAP Domain {0} and associated users of one and devices of one are deleted  
PAM-CMN-1669 = Run Port Scan on IP address: {0}. Ports: {1}  
PAM-CMN-1670 = Error resolving {0}  
PAM-CMN-1671 = Run nslookup on host {0}  
PAM-CMN-1672 = Problem starting SNMP Agent  
PAM-CMN-1673 = User {0} using API key {1} can't perform {2} operations while cluster is stopped. {3} was not executed.  
PAM-CMN-1674 = Invalid login name {0}.  
PAM-CMN-1675 = User {0} using API key {1} can't perform {2} operations while cluster is stopped. {3} was not executed.  
PAM-CMN-1676 = API key {0} not found for user {1}.  
PAM-CMN-1677 = SNMP Agent started successfully  
PAM-CMN-1678 = API key {0} for user {1} is inactive.  
PAM-CMN-1679 = Problem stopping SNMP Agent  
PAM-CMN-1680 = SNMP Agent stopped successfully  
PAM-CMN-1681 = User {0} is disabled. Unable to log on with API key {1}.  
PAM-CMN-1682 = Can not save SNMP daemon configuration!  
PAM-CMN-1683 = SNMP poll configuration saved successfully. Read-only Community: {0}  
PAM-CMN-1684 = User {0} using API key {1} can't log in while maintenance mode is enabled. {2} called by HTTP {3} was not executed. Please check with an administrator for further details  
PAM-CMN-1685 = User {0} using API key {1} called {2} via HTTP {3}  
PAM-CMN-1686 = Problem changing the SNMP Agent startup flag!  
PAM-CMN-1687 = SNMP Agent startup flag changed successfully. Start at boot: on  
PAM-CMN-1688 = SNMP Agent startup flag changed successfully. Start at boot: off  
PAM-CMN-1689 = Unable to build privilege manager for user {0} and API key {1}. Request was {2} via HTTP {3}  
PAM-CMN-1690 = Incorrect password for {0} external API user for {1}. Request was {2} via HTTP {3}  
PAM-CMN-1691 = Can not save SNMP trap configuration!  
PAM-CMN-1692 = SNMP trap configuration saved successfully. Trap Community: {0}  
PAM-CMN-1693 = An attempt was made to access unlicensed External REST API  
PAM-CMN-1694 = An attempt was made to access deactivated External REST API  
PAM-CMN-1695 = SNMPv3 Username "{0}" not found!  
PAM-CMN-1696 = Can not delete SNMPv3 user "{0}"!  
PAM-CMN-1697 = SNMPv3 Username "{0}" deleted successfully!  
PAM-CMN-1698 = Credential Service daemon is either not running or not reachable  
PAM-CMN-1699 = An attempt was made to access unlicensed External REST API documentation  
PAM-CMN-1700 = An attempt was made to access deactivated External REST API documentation  
PAM-CMN-1701 = Unauthorized access to service controller.  
PAM-CMN-1702 = Unauthorized access to External API Documentation  
PAM-CMN-1703 = Unauthorized access to External API Documentation: The user is not a global admin nor has API keys assigned.  
PAM-CMN-1704 = Downloaded Certificate {0}  
PAM-CMN-1705 = Downloaded CSR {0}  
PAM-CMN-1706 = Downloaded private key file {0}  
PAM-CMN-1707 = Uploaded Certificate {0}  
PAM-CMN-1708 = Certificate Upload: {0} ({1})  
PAM-CMN-1709 = Unable to retrieve host name for username {0}. Transparent Login for window '{1}' will not work.  
PAM-CMN-1710 = Error shortening url. Message was: {0}  
PAM-CMN-1711 = Problem with credential when logging. Launch aborted.  
PAM-CMN-1712 = No source IP address found for AWS API Proxy request.  
PAM-CMN-1713 = Invalid source IP address {0} found for AWS API Proxy request.

PAM-CMN-1714 = AWS API Proxy request came from IP address {0}, which is not on any whitelist.  
PAM-CMN-1715 = AWS API Proxy request for user {0} failed due to authentication failure. See previous log messages for details.  
PAM-CMN-1716 = Completely unexpected result was returned for Authentication Service for AWS proxy login. Returned value was {0}  
PAM-CMN-1717 = AWS API Proxy user {0} was not logged in because they do not have the AWS API Proxy user privilege  
PAM-CMN-1718 = No policy found connecting {0} and {1}  
PAM-CMN-1719 = Problems communicating with AWS. Message was {0}  
PAM-CMN-1720 = Unable to create target account for API key {0}-{1}. Message was {2}.  
PAM-CMN-1721 = API key {0} not found. Delete aborted.  
PAM-CMN-1722 = API key {0} deleted  
PAM-CMN-1723 = API key {0} was already deleted.  
PAM-CMN-1724 = Uploaded Certificate with Private Key {0}  
PAM-CMN-1725 = Uploaded Intermediate Certificate {0}  
PAM-CMN-1726 = Uploaded CA Bundles {0}  
PAM-CMN-1727 = Uploaded Certificate Revocation List {0}  
PAM-CMN-1728 = There is invalid CRL URL format: {0}  
PAM-CMN-1729 = There is invalid CRL file: {0}  
PAM-CMN-1730 = CRL file: {0} was added.  
  
PAM-CMN-1733 = External REST API Access has been enabled  
PAM-CMN-1734 = External REST API Access has been disabled  
PAM-CMN-1735 = External Password Authority API Access has been enabled  
PAM-CMN-1736 = External Password Authority API Access has been disabled  
PAM-CMN-1737 = {0} deleted successfully  
PAM-CMN-1738 = Unable to delete {0}  
PAM-CMN-1739 = Problem updating system certification to {0}  
PAM-CMN-1740 = Updated system certificate to {0}  
PAM-CMN-1741 = Command String has been enabled  
PAM-CMN-1742 = Command String has been disabled  
PAM-CMN-1743 = Config Password updated successfully  
PAM-CMN-1744 = Failed to delete target account for api key {0}  
PAM-CMN-1745 = Failed to retrieve target server for policy.  
  
PAM-CMN-1750 = Unknown device state name {0} code {1} for {2}  
  
PAM-CMN-1759 = Could not find domain name or ip address for {0}. Device is not added  
  
PAM-CMN-1764 = Invalid data supplied when reconciling device groups  
PAM-CMN-1765 = Unexpected provision type when reconciling device group {0}  
  
PAM-CMN-1767 = Duplicate address {0} for device {1}. Device not added.  
PAM-CMN-1768 = Unable to retrieve virtual device {0}, so skipping update.  
PAM-CMN-1769 = New address would result in duplicate domain name {0} for device {1}. Device is not updated.  
PAM-CMN-1770 = Proxy deactivation request came from IP {0}, which is not on any whitelist.  
PAM-CMN-1771 = Error deactivating device - {0}: {1}  
PAM-CMN-1772 = Successfully deactivated device {0}  
PAM-CMN-1773 = Attempt to deactivate by {0} is failed because it does not exist in the system.  
PAM-CMN-1774 = Added Transparent Login Configuration {0}  
PAM-CMN-1775 = Updated Transparent Login Configuration {0}  
PAM-CMN-1776 = Deleted Transparent Login Configuration {0}  
PAM-CMN-1777 = Unexpected sourceIP restriction value {0}. Value was ignored  
  
PAM-CMN-1790 = No policy found connecting {0} and {1}.  
PAM-CMN-1791 = Attempt to add target server {0} outside of licensing when Password Authority is not configured.

PAM-CMN-1792 = Unresolvable device conflict. Target server {0} wants to use the same domain/host name as the device {1}

PAM-CMN-1793 = Unable to find GK user {0}

PAM-CMN-1794 = Unable to find PA user {0}

PAM-CMN-1795 = Unable to find changed PA user {0}

PAM-CMN-1796 = Unable to update password for PA user {0}

PAM-CMN-1797 = Unable to reset password for PA user {0}. Error was {1}

PAM-CMN-1798 = Could not rename user {0}. Error was {1}

PAM-CMN-1799 = Successfully changed PA user {0} to {1}

PAM-CMN-1800 = Failed to execute searchUser command for {0}

PAM-CMN-1801 = Target Server not retrieved from Password Authority. Error Message {0}

PAM-CMN-1802 = Failed to retrieve id from request server {0}

PAM-CMN-1804 = Unable to retrieve Password Authority target account for username {0}. See previous log message for details.

PAM-CMN-1805 = Unable to retrieve Password Authority target account for username {0}. Error: {1}

PAM-CMN-1806 = Password view request returned warning code {0}. Message was {1}. Request ignored.

PAM-CMN-1807 = Unable to retrieve Password Authority password for username {0}. See previous log message for details

PAM-CMN-1808 = Unable to retrieve Password Authority password for username {0}. Error: {1}

PAM-CMN-1809 = Could not generate PA Username for GK user name {0}

PAM-CMN-1810 = Duplicate Password Authority username {0}. User not added

PAM-CMN-1811 = Missing required fields to delete target account. Hostname = {0} Application name = \${1} and username = {2}

PAM-CMN-1812 = Target account {0} for API key was already deleted or never existed. Proceeding as though the delete were successful.

PAM-CMN-1815 = Unable to locate {0} of type {1} belonging to {2}

PAM-CMN-1816 = Unable to find target server with id = {0} when looking for credentials

PAM-CMN-1823 = Unable to locate Password View Policy for dual auth view request - defaulting to 60 minute request interval.

PAM-CMN-1827 = Duplicate role name {0} not added.

PAM-CMN-1828 = Duplicate User Group {0} not added.

PAM-CMN-1829 = Unable to find privilege manager in session while trying to get list of user groups

PAM-CMN-1830 = Attempt to promote/demote user {0} to credential user group {1} failed. Group not found.

PAM-CMN-1831 = Unable to find pa user id for user {0}

PAM-CMN-1832 = Could not get details on credentials management user groups for user {0}

PAM-CMN-1833 = Could not get details on credentials management roles for user {0}

PAM-CMN-1834 = Could not get credentials management user groups for user {0}

PAM-CMN-1835 = API key {0} has privileges in excess of its user {1}. Login not allowed.

PAM-CMN-1836 = User {0} using API key {1} can't perform {2} operations on private API methods in this configuration. {3} was not executed.

PAM-CMN-1868 = {0} user already exists, was not changed.

PAM-CMN-1869 = Cannot remove {0} license feature. Please remove custom user roles with {0} privilege

PAM-CMN-1870 = Cannot remove {0} license feature. Please remove CA TAP API User role from the following users: {1}

PAM-CMN-1871 = Cannot remove {0} license feature while users still have API client keys.

PAM-CMN-1872 = An error occurred saving CA Threat Analytics configuration.

PAM-CMN-1873 = An error occurred clearing CA Threat Analytics configuration.

PAM-CMN-1874 = Maintenance mode has been enabled for this appliance

PAM-CMN-1875 = Maintenance mode has been disabled for this appliance

PAM-CMN-1876 = Failed to create target application {0}

PAM-CMN-1877 = Cannot remove External API license feature while users still have API client keys.

PAM-CMN-1885 = Updated active flag for {0} region {1} to {2}

PAM-CMN-1887 = Invalid refresh interval {0}. No change was made.

PAM-CMN-1910 = Updated CRL download interval to {0}

PAM-CMN-1911 = Disabled CRL download schedule

PAM-CMN-1912 = Restarting Apache Web Server

PAM-CMN-1913 = Downloaded database file {0}

PAM-CMN-1914 = S3 mounting performed successfully

PAM-CMN-1915 = Unmounting performed successfully

PAM-CMN-1916 = Unmount operation unsuccessful.

PAM-CMN-1917 = Database file {0} deleted successfully.

PAM-CMN-1918 = Unable to load PAM certificate for SSO user {0}. User will not be able to log-in

PAM-CMN-1919 = Remote CA-PAM Debugging Services turned {0}

PAM-CMN-1925 = Created Self-Signed Certificate {0}

PAM-CMN-1926 = Created CSR {0}

PAM-CMN-1927 = Missing required information for launch. Missing device id, RDP application {0}. User {1}

PAM-CMN-1928 = Message for device {0}: {1}

PAM-CMN-1930 = Device is marked as a target server, but no target server exists. Please set the value of the Password Management check box as you wish and click OK.

PAM-CMN-1931 = Device is marked as a request client, but no request client exists. Please set the value of the A2A check box as you wish and click OK.

PAM-CMN-1964 = Sending Password Authority subsystem start command to member {0} (ELAPSED TIME = {1}) ...

PAM-CMN-1965 = Password Authority subsystem started on node {0} (ELAPSED TIME = {1})

PAM-CMN-1979 = {0}: failed: {1}

PAM-CMN-1980 = {0} restarted

PAM-CMN-1996 = CPU temperature has recovered.

PAM-CMN-1997 = Chassis fan has recovered.

PAM-CMN-1998 = Primary drive has recovered.

PAM-CMN-1999 = Secondary drive has recovered.

PAM-CMN-2000 = Primary (leftmost) power supply unit has recovered.

PAM-CMN-2001 = Secondary (rightmost) power supply unit has recovered.

PAM-CMN-2002 = CPU temperature is higher than 134 degrees Fahrenheit!

PAM-CMN-2003 = Chassis fan has failed!

PAM-CMN-2004 = Primary drive has failed!

PAM-CMN-2005 = Secondary drive has failed!

PAM-CMN-2006 = Primary (leftmost) power supply unit has failed!

PAM-CMN-2007 = Secondary (rightmost) power supply unit has failed!

PAM-CMN-2059 = gkmonitor[{0}]: {1}--{2} {3}--Failed {4}

PAM-CMN-2060 = gkmonitor[{0}]: {1}--{2} {3}--Succeeded {4}

PAM-CMN-2061 = gkmonitor[{0}]: {1}--{2} {3}--{4}

PAM-CMN-2062 = gkmonitor[{0}]: {1}

PAM-CMN-2063 = gkmonitor[{0}]: Unable to send email! {1} email configuration is incorrect!

PAM-CMN-2064 = gkmonitor[{0}]: {1} started

PAM-CMN-2065 = gkmonitor[{0}]: {1} terminated

PAM-CMN-2066 = gkmonitor[{0}]: Monitor Parameter {1} has an empty value ... Exiting !

PAM-CMN-2067 = {0}: Received Error {1}

PAM-CMN-2068 = Connection Restored to the Database

PAM-CMN-2069 = Unable to create session log

PAM-CMN-2070 = Logged {0} event from client. Return status was {1}.



PAM-CMN-2071 = Invalid userId {0} for get DbRiskLevel. No risk level will be returned.

PAM-CMN-2072 = Malformed or invalid JSON when posting a {0} event to {1}. Http response code is {2}.

PAM-CMN-2073 = Malformed or invalid JSON when posting a {0} event to {1}. Http response code is {2}. Status was {3} .

PAM-CMN-2074 = Malformed or invalid JSON when posting a {0} event to {1}. Http response code is {2}. Status message was {3}.

PAM-CMN-2075 = Malformed or invalid JSON when posting a {0} event to {1}. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2076 = Not authorized to connect to {0} during {1} event. Http response code is {2}.

PAM-CMN-2077 = Not authorized to connect to {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2078 = Not authorized to connect to {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2079 = Not authorized to connect to {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2080 = Forbidden to connect to {0} during {1} event. Http response code is {2}.

PAM-CMN-2081 = Forbidden to connect to {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2082 = Forbidden to connect to {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2083 = Forbidden to connect to {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2084 = Resource or nested resource not found in {0} during {1} event. Http response code is {2}.

PAM-CMN-2085 = Resource or nested resource not found in {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2086 = Resource or nested resource not found in {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2087 = Resource or nested resource not found in {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2088 = Request method not allowed in {0} during {1} event. Http response code is {2}.

PAM-CMN-2089 = Request method not allowed in {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2090 = Request method not allowed in {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2091 = Request method not allowed in {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2092 = Too many requests to connect to {0} during {1} event. Http response code is {2}.

PAM-CMN-2093 = Too many requests to connect to {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2094 = Too many requests to connect to {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2095 = Too many requests to connect to {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2096 = Server error on connection to {0} during {1} event. Http response code is {2}.

PAM-CMN-2097 = Server error on connection to {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2098 = Server error on connection to {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2099 = Server error on connection to {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2100 = {0} temporarily unavailable during {1} event. Http response code is {2}.

PAM-CMN-2101 = {0} temporarily unavailable during {1} event. Http response code is {2}. Status was {3}.

PAM-CMN-2102 = {0} temporarily unavailable during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2103 = {0} temporarily unavailable during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2104 = Unable to connect to {0} during {1} event. Http response code is {2}.

PAM-CMN-2105 = Unable to connect to {0} during {1} event. Http response code is {2}. Status was {3} .

PAM-CMN-2106 = Unable to connect to {0} during {1} event. Http response code is {2}. Status message was {3}.

PAM-CMN-2107 = Unable to connect to {0} during {1} event. Http response code is {2}. Status was {3} . Status message was {4}.

PAM-CMN-2108 = Privilege manager not found in session - risk levels not reset.

PAM-CMN-2109 = User {0} tried to set risk levels for user {1} without authorization.

PAM-CMN-2110 = Invalid user id {0}. User risk level was not changed.  
 PAM-CMN-2111 = No user found for user id {0}. User risk level was not changed.  
 PAM-CMN-2112 = Invalid risk level {0}. Risk level not changed.  
 PAM-CMN-2113 = User {0}'s risk level was changed to {1}.  
 PAM-CMN-2114 = Privilege manager not found in session.  
 PAM-CMN-2115 = Created {0} API user {1} with user id {2}.  
 PAM-CMN-2116 = Invalid risk level value {0}. User risk level not added.  
 PAM-CMN-2117 = Deleted {0} API user {1}.  
 PAM-CMN-2118 = Session id was not in proper format. Can't start recording active connections  
 PAM-CMN-2119 = Applying mitigations to user: {0}.  
 PAM-CMN-2120 = Invalid user id {0} specified for apply mitigation for user. No mitigations were applied.  
  
 PAM-CMN-2123 = Failed to close remote factories. Exception was {0}. Message was {1}.  
 PAM-CMN-2124 = Problem with PAM {0}, {1}  
 PAM-CMN-2125 = Test from PAM {0}, process {1}  
 PAM-CMN-2126 = This is a test from the PAM Monitor to make sure mail is working properly, and is also an indication that the PAM Monitor is attempting to be started.  
 PAM-CMN-2127 = Licensing Message from PAM Instance '{0}'  
 PAM-CMN-2128 = <br/><br/>The following message from the PAM license monitor on PAM instance:<br/><br/> {0}<br/><br/>requires your attention. Please review the message below and see the logs on your CA PAM instance for further information<br/><br/> {1}<br/>  
 PAM-CMN-2129 = Message from PAM {0}, Host {1}  
 PAM-CMN-2130 = \*\*\*\*\*ERROR\*\*\*\*\*ERROR\*\*\*\*\*<br/>{0}  
 PAM-CMN-2131 = \*\*\*\*\*INFORMATION\*\*\*\*\*<br/>{0}  
  
 PAM-CMN-2134 = No users are disabled in PAM.  
 PAM-CMN-2135 = Disabled user account: {0} removed from PAM  
 PAM-CMN-2137 = Error generating credentials for database backup!  
 PAM-CMN-2138 = No remote server specified!  
 PAM-CMN-2139 = Unable to backup CA PAM database!  
 PAM-CMN-2140 = Unable to backup CA PAM configuration!  
 PAM-CMN-2141 = Error uploading {0} to {1}!  
 PAM-CMN-2142 = Specified mount {0} is down!  
 PAM-CMN-2143 = Protocol not specified for database and configuration backup scheduler!  
 PAM-CMN-2144 = Scheduled backup files {0} and {1} sent to {2}  
 PAM-CMN-2145 = DB compact already in progress!  
 PAM-CMN-2146 = Place system in maintenance mode before compacting the database  
 PAM-CMN-2147 = A fatal error occurred while dumping the database for the DB compact.  
 PAM-CMN-2148 = An error occurred while saving the database dump for compacting.  
 PAM-CMN-2149 = An error occurred while dropping the database for the database compacting.  
 PAM-CMN-2150 = A fatal error occurred while restoring the database for the DB compact, {0}.  
 PAM-CMN-2151 = PAM databases have been compacted.  
 PAM-CMN-2152 = Too many instances of [rotate\\_coredumps.pl](#) running  
 PAM-CMN-2153 = Found {0} memory dumps  
 PAM-CMN-2154 = Found {0} memory dumps, pruned {1}  
 PAM-CMN-2155 = Failed to push new {0} risk level for user to {1}. Exception was {2}. Message was {3}.  
 PAM-CMN-2156 = Logged {0} event from device {1}. Return status was {2}.  
 PAM-CMN-2157 = Logged {0} event from device {1} for reason {2}. Return status was {3}.  
  
 PAM-CMN-2165 = Unauthorized word {0} typed.  
 PAM-CMN-2166 = No email contact to alert.  
 PAM-CMN-2167 = Exceeded the maximum number of allowed violations. Session terminated.  
 PAM-CMN-2168 = The value for sortBy must begin with either + for ascending sort or - for descending sort. Make sure to URL encode the + symbol.

PAM-CMN-2169 = External API not licensed. Authentication refused.  
PAM-CMN-2170 = Authentication required.  
PAM-CMN-2171 = External API may not be used when the cluster is stopped. Please check with an administrator for further details.  
PAM-CMN-2172 = Not Found  
PAM-CMN-2173 = The attempt to retrieve the user's password for login failed. Please check with an administrator for further details.  
PAM-CMN-2174 = User {0} can't login while maintenance mode is enabled.  
PAM-CMN-2175 = Unable to build privilege manager for user {0} and API key {1}.  
  
PAM-CMN-2187 = Unable to retrieve credential for getting the role token.  
PAM-CMN-2188 = Unable to retrieve credential for getting the role token. Message was {0}  
PAM-CMN-2189 = Couldn't change {0}.  
PAM-CMN-2190 = API Key target server. All api key target accounts are associated with this device.  
PAM-CMN-2191 = Policy id must be a positive integer.  
PAM-CMN-2192 = Updated policy.  
PAM-CMN-2193 = Created policy.  
PAM-CMN-2194 = User: {0};  
PAM-CMN-2195 = Host: {0};  
PAM-CMN-2196 = Credential(s): {0};  
PAM-CMN-2197 = Services  
PAM-CMN-2198 = Policy: {0}  
  
PAM-CMN-2200 = Filtering  
PAM-CMN-2201 = Command Filtering: off;  
PAM-CMN-2202 = Command Filtering: black-list: {0};  
PAM-CMN-2203 = Command Filtering: white-list: {0};  
PAM-CMN-2204 = Socket Filtering: black-list: {0};  
PAM-CMN-2205 = Socket Filtering: white-list: {0};  
PAM-CMN-2206 = Socket Filtering: off;  
  
PAM-CMN-2215 = User's access to service {0} on device {1} disabled due to {2} conflicts. The conflicting associations are between  
PAM-CMN-2216 = User's access to access method {0} on device {1} disabled due to {2} conflicts. The conflicting associations are between  
PAM-CMN-2217 = User/Group {0} and Device/Group {1}  
  
PAM-CMN-2220 = Command filter white lists are ignored for Mainframe Access Methods;  
PAM-CMN-2221 = Transparent Login: on;  
PAM-CMN-2222 = Transparent Login: off;  
PAM-CMN-2223 = Server Control Login: on;  
PAM-CMN-2224 = Server Control Login: off;  
PAM-CMN-2225 = Kerberos KDC server connection for host: {0}.  
  
PAM-CMN-2229 = The device {0} has more than one target account defined for command string transparent login.  
PAM-CMN-2230 = The target account {0} belonging to target application {1} on the device {2} is used by the users/groups  
PAM-CMN-2231 = Service is disabled until the conflict is resolved.  
PAM-CMN-2232 = Applet is disabled until the conflict is resolved.  
PAM-CMN-2233 = User group {0} successfully added. {1}  
PAM-CMN-2234 = Unknown error on multi user group delete {0}  
PAM-CMN-2235 = Unrecognized return type from delete of user group {0} response was {1}  
PAM-CMN-2236 = Unknown error on multi user delete {0}  
PAM-CMN-2237 = Virtual user {0} successfully added.  
PAM-CMN-2238 = User {0} successfully added.  
PAM-CMN-2239 = Activation: Now;



PAM-CMN-2251 = Activation: {0};  
PAM-CMN-2252 = Expiration: Never;  
PAM-CMN-2253 = Expiration: {0};  
PAM-CMN-2254 = User {0} successfully deleted. {1}  
PAM-CMN-2255 = Local IP: {0};  
PAM-CMN-2256 = Ports: {0};  
PAM-CMN-2257 = Protocol: {0};  
PAM-CMN-2258 = Application Protocol: Disabled;  
PAM-CMN-2259 = Application Protocol: {0};  
PAM-CMN-2260 = Target Server {0} is not added to Password Authority. Error Message: {1};  
PAM-CMN-2261 = Password Authority failure to try to activate user {0}. Message: {1}.  
PAM-CMN-2262 = PA User {0} not updated. Error message: {1}.  
PAM-CMN-2263 = Target Server {0} is not updated. Error message: {1}.  
PAM-CMN-2264 = Target server search failed. Error message: {0}.  
PAM-CMN-2265 = Target Server {0} is not deleted. Reason: {0}.  
PAM-CMN-2266 = Request Server not retrieved from Password Authority. Error Message: {0}.  
PAM-CMN-2267 = Request Server is not added to Password Authority. Error Message: {0}.  
PAM-CMN-2268 = Request server {0} is not updated. Error message: {1}.  
PAM-CMN-2269 = Request Server {0} is not deleted. Reason: {1}.  
PAM-CMN-2270 = searchUser request for {0} failed. Error Message: {1}.  
PAM-CMN-2271 = User {0} is not found in Password Authority.  
PAM-CMN-2272 = User {0} is not deleted from Password Authority. Error Message: {1}.  
PAM-CMN-2273 = User {0} is deleted from Password Authority.  
PAM-CMN-2274 = Unable to retrieve Password Authority target account for username {0}. Error: {1}.  
PAM-CMN-2275 = Unable to retrieve Password Authority password for username {0}. Error: {1}.  
  
PAM-CMN-2277 = User {0} is not added to Password Authority - error was {1}.  
PAM-CMN-2278 = Could not successfully retrieve Password Authority Managed Data for Dashboard. Error: {0}  
PAM-CMN-2279 = Unable to delete target account {0} for API Key - error was {1}.  
  
PAM-CMN-2282 = Unable to retrieve target account list for policies - error was {0}.  
PAM-CMN-2283 = Unable to retrieve target account list - error was {0}.  
PAM-CMN-2284 = Web Portal Launch URL: {0};  
PAM-CMN-2285 = Browser Type: {0};  
PAM-CMN-2286 = Access List: {0};  
PAM-CMN-2287 = Error when attempting to retrieve password view requests - error was {0}.  
PAM-CMN-2288 = Client Application: {0};  
PAM-CMN-2289 = Enabled: on;  
PAM-CMN-2290 = Enabled: off;  
PAM-CMN-2291 = Service {0} added successfully. {1}  
PAM-CMN-2292 = Service {0} updated successfully. {1}  
PAM-CMN-2293 = A Password Authority problem prevented completing the request. Error when attempting to retrieve password view requests. Check log for details.  
PAM-CMN-2294 = Unknown error on multi service delete {0}  
PAM-CMN-2295 = {0} SSL VPN service(s) deleted, {1} SSL VPN service(s) not deleted for lack of privilege, {2} SSL VPN service(s) not found, {3} unknown SSL VPN service delete errors  
PAM-CMN-2296 = {0} service(s) deleted, {1} service(s) not deleted for lack of privilege, {2} service(s) not found, {3} unknown service delete errors  
PAM-CMN-2297 = Reenabled {0} user(s): {1}  
PAM-CMN-2298 = {0} users were requested to be enabled, {1} users were actually enabled: {2}  
PAM-CMN-2299 = Error when attempting to retrieve target account with ID {0} - error was {1}.  
PAM-CMN-2300 = Error when attempting to retrieve target account with device Name {0}, target application name {1}, user name {2} - error was {3}.  
PAM-CMN-2301 = Error when attempting to update a password view request status - error was {0}.

PAM-CMN-2302 = Error when attempting to retrieve pa user id via access user id - error was {0}.  
PAM-CMN-2303 = Error when attempting to retrieve password composition policies - error was {0}.  
PAM-CMN-2304 = Error when attempting to retrieve ssh key pair policies - error was {0}.  
PAM-CMN-2305 = Error when attempting to add target account for username {0} - error was {1}.  
PAM-CMN-2306 = Error when attempting to update target account for username {0} - error was {1}.  
PAM-CMN-2307 = Error when attempting to check in password - error was {0}.  
PAM-CMN-2308 = Error when attempting to retrieve target application domain name - error was {0}.  
PAM-CMN-2309 = Error when attempting to locate master target application - error was {0}.  
PAM-CMN-2310 = Unable to retrieve EC2 shared keypair names - error was {0}.  
PAM-CMN-2311 = Error when attempting to retrieve account name - error was {0}.  
PAM-CMN-2312 = Error when trying to find target server id with name {0} - error was {1}.

PAM-CMN-2318 = Unable to delete target group from Password Authority. Error Message: Call to deleteDynamicGroup with neither groupId nor groupName specified.  
PAM-CMN-2319 = Unable to delete request group from Password Authority. Error Message: Call to deleteDynamicGroup with neither groupId nor groupName specified.  
PAM-CMN-2320 = Unable to delete target group {0} from Password Authority. Error Message: Group name {1} and group id {2} did not match.  
PAM-CMN-2321 = Unable to delete request group {0} from Password Authority. Error Message: Group name {1} and group id {2} did not match.  
PAM-CMN-2322 = Attempt to rotate password failed - error was {0}.  
PAM-CMN-2323 = Missing required field: name for role.  
PAM-CMN-2324 = Missing required field: permissions for role..  
PAM-CMN-2325 = Missing required field: name for user group..  
PAM-CMN-2326 = Missing required field: role id for user group..  
PAM-CMN-2327 = Missing required field: Command String.  
PAM-CMN-2328 = Synchronized time with Time Servers  
PAM-CMN-2329 = Time synchronization failed after 2 attempts!<br>Please, try again in a few seconds  
PAM-CMN-2330 = Error updating Time Servers information.  
PAM-CMN-2331 = Updated Time Servers. Synchronize at boot: Enabled, Servers: {0}  
PAM-CMN-2332 = Updated Time Servers. Synchronize at boot: Disabled, Servers: {0}  
PAM-CMN-2333 = Date/Time changed successfully. New time: {0} in Timezone: {1}.  
PAM-CMN-2334 = Unable to change Date/Time.  
PAM-CMN-2335 = Target Server {0} is added to Password Authority.  
PAM-CMN-2336 = Target server {0} is updated.  
PAM-CMN-2337 = Restarting Apache Web Server  
PAM-CMN-2338 = Downloaded database file {0}  
PAM-CMN-2339 = S3 mounting performed successfully  
PAM-CMN-2340 = Unmounting performed successfully  
PAM-CMN-2341 = Unmount operation unsuccessful.  
PAM-CMN-2342 = Database file {0} deleted successfully.  
PAM-CMN-2343 = Unable to load PAM certificate for SSO user {0}. User will not be able to log-in  
PAM-CMN-2344 = Remote CA-PAM Debugging Services turned {0}  
  
PAM-CMN-2350 = Created Self-Signed Certificate {0}  
PAM-CMN-2351 = Created CSR {0}  
PAM-CMN-2352 = Target server {0} is deleted.

PAM-CMN-2355 = Missing required information for launch. Device {0} Missing id of what to launch (no task, service, or rdp application Id. User {1}  
PAM-CMN-2356 = Missing required information for launch. Device {0}, task {1}, service {2}, RDP application {3}. User {4}  
PAM-CMN-2357 = Missing required information for launch. Device {0}, service {1}, RDP application {2}. User {3}  
PAM-CMN-2358 = Missing required information for launch. Device {0}, task {1}, service {2}. User {3}  
PAM-CMN-2359 = Missing required information for launch. Device {0}, task {1}, RDP application {2}. User {3}

PAM-CMN-2360 = Missing required information for launch. Device {0}, task {1}. User {2}  
PAM-CMN-2361 = Missing required information for launch. Device {0}, service {1}. User {2}  
PAM-CMN-2362 = Missing required information for launch. Device {0}, RDP application {1}. User {2}  
PAM-CMN-2363 = Missing required information for launch. Missing device id Missing id of what to launch (no task, service, or rdp application Id. User {0}  
PAM-CMN-2364 = Missing required information for launch. Missing device id, task {0}, service {1}, RDP application {2}. User {3}  
PAM-CMN-2365 = Missing required information for launch. Missing device id, service {0}, RDP application {1}. User {2}  
PAM-CMN-2366 = Missing required information for launch. Missing device id, task {0}, service {1}. User {2}  
PAM-CMN-2367 = Missing required information for launch. Missing device id, task {0}, RDP application {1}. User {2}  
PAM-CMN-2368 = Missing required information for launch. Missing device id, task {0}. User {1}  
PAM-CMN-2369 = Missing required information for launch. Missing device id, service {0}. User {1}  
PAM-CMN-2370 = Request server {0} is updated  
PAM-CMN-2372 = User {0} successfully updated.  
PAM-CMN-2373 = Account disabled;  
PAM-CMN-2374 = Account enabled;  
PAM-CMN-2375 = SSL VPN Service {0} added successfully.  
PAM-CMN-2376 = SSL VPN Service {0} added successfully. TCP Ports: {1};  
PAM-CMN-2377 = SSL VPN Service {0} added successfully. UDP Ports: {1};  
PAM-CMN-2378 = SSL VPN Service {0} added successfully. TCP Ports: {1}; UDP Ports: {2};  
PAM-CMN-2379 = SSL VPN Service {0} updated successfully.  
PAM-CMN-2380 = SSL VPN Service {0} updated successfully. TCP Ports: {1};  
PAM-CMN-2381 = SSL VPN Service {0} updated successfully. UDP Ports: {1};  
PAM-CMN-2382 = SSL VPN Service {0} updated successfully. TCP Ports: {1}; UDP Ports: {2};  
PAM-CMN-2383 = Unable to add user {0}  
PAM-CMN-2384 = Service {0} added successfully.  
PAM-CMN-2385 = Service {0} added successfully. Launch Path: {1};  
PAM-CMN-2386 = Service {0} added successfully. Enabled: {1};  
PAM-CMN-2387 = Service {0} added successfully. Launch Path: {1}; Enabled: {2};  
PAM-CMN-2388 = Service {0} updated successfully.  
PAM-CMN-2389 = Service {0} updated successfully. Launch Path: {1};  
PAM-CMN-2390 = Service {0} updated successfully. Enabled: {1};  
PAM-CMN-2391 = Service {0} updated successfully. Launch Path: {1}; Enabled: {2};  
PAM-CMN-2392 = restrictDelete was not set for provision row for vCenter authorization server {0} and user {1}. Url was {2} Message was {3}  
PAM-CMN-2393 = Unable to retrieve vCenter target server information.  
PAM-CMN-2394 = Unable to retrieve vCenter target server information. Message was unable to retrieve vCenter target server information.  
PAM-CMN-2395 = {0} Connection aborted.  
PAM-CMN-2396 = {0} Attempting to connect anyway.  
PAM-CMN-2397 = {0} Could not retrieve device information from PAM.  
PAM-CMN-2398 = Roles: None;  
PAM-CMN-2399 = Roles: {0};  
  
PAM-CMN-2405 = Error adding ldap group: {0}  
PAM-CMN-2406 = Access methods: {0};  
PAM-CMN-2407 = Access methods: None;  
PAM-CMN-2408 = Services: {0};  
PAM-CMN-2409 = Services: None;  
PAM-CMN-2410 = VPN Services: {0};  
PAM-CMN-2411 = VPN Services: None;  
PAM-CMN-2412 = Credential sources removed;  
PAM-CMN-2413 = Credential sources: {0};

PAM-CMN-2414 = Tags: {0};  
PAM-CMN-2415 = Tags: None;  
PAM-CMN-2416 = Device Group {0} added successfully.  
PAM-CMN-2417 = Unknown error on multi device group delete {0}  
PAM-CMN-2418 = Unrecognized return type from delete of device group {0}  
PAM-CMN-2419 = Group {0} updated successfully. Devices in group updated.  
PAM-CMN-2420 = New name: {0};  
PAM-CMN-2421 = Group description updated;  
PAM-CMN-2422 = Provision type updated;  
PAM-CMN-2423 = Password push flag updated;  
PAM-CMN-2424 = Legal Notice flag updated;  
PAM-CMN-2425 = Groups: None;  
PAM-CMN-2426 = Groups: {0};  
PAM-CMN-2427 = Runtime update automatically updated virtual device.  
PAM-CMN-2428 = Runtime update automatically updated virtual device. address: {0}  
PAM-CMN-2429 = Runtime update automatically updated virtual device. status: active  
PAM-CMN-2430 = Runtime update automatically updated virtual device. status: inactive  
PAM-CMN-2431 = Runtime update automatically updated virtual device. address: {0} status: active  
PAM-CMN-2432 = Runtime update automatically updated virtual device. address: {0} status: inactive  
PAM-CMN-2433 = Unknown error on multi device delete {0} for device id {1}  
PAM-CMN-2434 = Device {0} successfully deleted. {1} {2}  
PAM-CMN-2435 = Transparent logins: {0}  
PAM-CMN-2436 = Transparent Logins were deleted.  
PAM-CMN-2437 = Device {0} added successfully.  
PAM-CMN-2438 = Unable to grant access to {0} because '{1}'  
PAM-CMN-2439 = {0} aborted. {1}  
PAM-CMN-2471 = Failed to retrieve user data for user {0}.  
PAM-CMN-2472 = Invalid OS {0} for target application.  
PAM-CMN-2473 = Invalid task for target application.  
PAM-CMN-2474 = Target application {0} on {1} is created.  
PAM-CMN-2475 = Target application {0} on {1} is not created. Reason: {2}.  
PAM-CMN-2476 = Request Server {0} is added to A2A via autoregistration.  
PAM-CMN-2477 = Request Server {0} is added to A2A.  
PAM-CMN-2478 = Request Server {0} is modified via autoregistration.  
PAM-CMN-2479 = Password Authority request server {0} is deleted.  
PAM-CMN-2480 = User {0} is added to PA with group membership: {1}.  
PAM-CMN-2481 = Target Application {0} was updated on device {1}.  
PAM-CMN-2482 = Target Application {0} was added to device {1}.  
PAM-CMN-2483 = Either name or ID must be specified to delete a user group.  
PAM-CMN-2484 = Request server {0} is updated. Request server name is changed to {1}.  
PAM-CMN-2485 = Operation failed because of unknown Password Authority error.  
PAM-CMN-2486 = GB{0} has come up.  
PAM-CMN-2487 = GB{0} has gone down!  
PAM-CMN-2488 = device inactive  
PAM-CMN-2489 = device deleted  
PAM-CMN-2490 = ok  
PAM-CMN-2491 = connection failure  
  
PAM-CMN-2495 = {0} virtual device scan completed for access key {1} region {2}. {3} devices added, {4} devices updated, {5} devices deleted.  
PAM-CMN-2496 = {0} virtual device scan completed for access key {1} region not found. {2} devices added, {3} devices updated, {4} devices deleted.

PAM-CMN-2497 = {0} virtual device scan completed for vCenter URL {1} user {2}. {3} devices added, {4} devices updated, {5} devices deleted.

PAM-CMN-2498 = {0} virtual device scan completed. {1} devices added, {2} devices updated, {3} devices deleted.

PAM-CMN-2499 = Device {0} had the same ip address {1} as the devices {2} and was not processed.

PAM-CMN-2500 = Device {0} had the same domain {1} as the devices {2} and was not processed.

PAM-CMN-2504 = Reported problem on NFS for DB backup

PAM-CMN-2506 = Reported problem with NFS share for DB Backup

PAM-CMN-2508 = Reported problem on Amazon S3 for DB backup

PAM-CMN-2510 = Reported problem on SMB for DB backup

PAM-CMN-2518 = {0} Exclusive-use account; Check-in time: {1}, Check-out time: {2}; by {3}

PAM-CMN-2519 = The device {0} has more than one target account defined for command string transparent login.

PAM-CMN-2520 = The target account {0} belonging to target application {1} on the device {2} is used by the users/groups.

PAM-CMN-2521 = Service is disabled until the conflict is resolved.

PAM-CMN-2522 = Applet is disabled until the conflict is resolved.

PAM-CMN-2523 = Keyword: {0} Alert: {1} Regex: {2} Block: {3};

PAM-CMN-2524 = On

PAM-CMN-2525 = Off

PAM-CMN-2526 = Command Filter List {0} Updated. Name: {1} Type: black Keywords: None;

PAM-CMN-2527 = Command Filter List {0} Updated. Name: {1} Type: white Keywords: None;

PAM-CMN-2528 = Command Filter List {0} Updated. Name: {1} Type: black Keywords: {2};

PAM-CMN-2529 = Command Filter List {0} Updated. Name: {1} Type: white Keywords: {2};

PAM-CMN-2530 = Command Filter List Created. Name: {0} Type: black Keywords: None;

PAM-CMN-2531 = Command Filter List Created. Name: {0} Type: white Keywords: None;

PAM-CMN-2532 = Command Filter List Created. Name: {0} Type: black Keywords: {1};

PAM-CMN-2533 = Command Filter List Created. Name: {0} Type: white Keywords: {1};

PAM-CMN-2534 = Socket Filter List Created. Name: {0} Type: black Hosts: None;

PAM-CMN-2535 = Socket Filter List Created. Name: {0} Type: white Hosts: None;

PAM-CMN-2536 = Socket Filter List Created. Name: {0} Type: black Hosts: {1};

PAM-CMN-2537 = Socket Filter List Created. Name: {0} Type: white Hosts: {1};

PAM-CMN-2538 = Socket Filter List {0} Updated. Name: {1} Type: black Hosts: None;

PAM-CMN-2539 = Socket Filter List {0} Updated. Name: {1} Type: white Hosts: None;

PAM-CMN-2540 = Socket Filter List {0} Updated. Name: {1} Type: black Hosts: {2};

PAM-CMN-2541 = Socket Filter List {0} Updated. Name: {1} Type: white Hosts: {2};

PAM-CMN-2542 = Command Filter Configuration Updated. Blacklist Violation Message: {0} Whitelist Violation Message: {1} Violation Additional e-mail Message: {2} Violations Before Action: {3} Action After Limit Exceeded: {4}

PAM-CMN-2543 = Socket Filter Configuration Updated. Agent Port: {0} SFA Monitoring: Enabled Appliance ID: {1} Violation Message: {2} Violation Additional e-mail Message: {3} Violations Before Action: {4} Action After Limit Exceeded: {5} Log All Access: Enabled

PAM-CMN-2544 = Socket Filter Configuration Updated. Agent Port: {0} SFA Monitoring: Enabled Appliance ID: {1} Violation Message: {2} Violation Additional e-mail Message: {3} Violations Before Action: {4} Action After Limit Exceeded: {5} Log All Access: Disabled

PAM-CMN-2545 = Socket Filter Configuration Updated. Agent Port: {0} SFA Monitoring: Disabled Appliance ID: {1} Violation Message: {2} Violation Additional e-mail Message: {3} Violations Before Action: {4} Action After Limit Exceeded: {5} Log All Access: Enabled

PAM-CMN-2546 = Socket Filter Configuration Updated. Agent Port: {0} SFA Monitoring: Disabled Appliance ID: {1} Violation Message: {2} Violation Additional e-mail Message: {3} Violations Before Action: {4} Action After Limit Exceeded: {5} Log All Access: Disabled

PAM-CMN-2550 = Transparent logins: None



PAM-CMN-2577 = Can't add Splunk server.  
PAM-CMN-2578 = Message {0}  
PAM-CMN-2583 = Full path  
PAM-CMN-2584 = Prompt  
PAM-CMN-2585 = users in group {0}  
PAM-CMN-2586 = users common to groups {0}  
PAM-CMN-2587 = devices in group {0}  
PAM-CMN-2588 = devices common to groups {0}  
PAM-CMN-2589 = Internal communication error  
  
PAM-CMN-2592 = {0} rows to move {1} actually moved.  
PAM-CMN-2593 = Could not find the group id for the group {0}  
PAM-CMN-2594 = Could not delete group members!  
PAM-CMN-2595 = Could not delete the group {0}  
  
PAM-CMN-2597 = You have not registered.  
PAM-CMN-2598 = You have configured this GateKeeper to Managed mode.  
PAM-CMN-2599 = Your Login has Timed Out.  
PAM-CMN-2600 = Email Alerted {0}: {1}  
PAM-CMN-2601 = CA Single Sign-On Web Agent disabled. For this change to take affect, please restart Apache.  
PAM-CMN-2602 = An error occured disabling CA Single Sign-On Weg Agent.  
  
PAM-CMN-2604 = No form exists  
PAM-CMN-2605 = Invalid port number! Please, enter a number between 1 and 65535!  
PAM-CMN-2606 = Database backup schedule saved successfully!  
PAM-CMN-2607 = Problem saving the database backup schedule:<br>{0}  
PAM-CMN-2608 = All calendar fields are required in this form!  
PAM-CMN-2609 = Need to specify an account to use for authentication  
PAM-CMN-2610 = Invalid database backup account - backup settings are not reset  
PAM-CMN-2611 = Unable to set database backup account!  
PAM-CMN-2612 = Unable to reset database values!  
PAM-CMN-2613 = Unable to connect: Code: {0}, Message: {1}  
PAM-CMN-2614 = Error connecting to the local listener!  
  
PAM-CMN-2615 = gatekeeper: {0} connected to {1}  
PAM-CMN-2616 = gatekeeper: {0} closed connection to {1}  
PAM-CMN-2617 = GB {0} has come up.  
PAM-CMN-2618 = GB {0} has come down.  
PAM-CMN-2620 = GK Auth system started on {0}:{1}  
PAM-CMN-2621 = Shutting down GK authentication engine  
  
PAM-CMN-2727 = Quitting CSPM due to critical failure.  
  
PAM-CMN-2740 = Only read-only REST methods (GET) are allowed on secondary sites.  
PAM-CMN-2741 = Update failed. Please try again later.  
PAM-CMN-2742 = My Info has been updated successfully, but your changes are pending.  
  
PAM-CMN-2748 = This CA-PAM appliance is a member of a secondary site. Most admin functions are disabled and must be performed from the primary site.  
PAM-CMN-2749 = Config user logged in successfully.  
PAM-CMN-2750 = Config user failed to log in.  
PAM-CMN-2751 = Deleting RADIUS user {0} failed: Unable to connect to the primary site ({1}) to delete the user.  
  
PAM-CMN-2807 = Partition status file does not exist  
  
PAM-CMN-2814 = No storage element for PAM on {0}  
  
PAM-CMN-2816 = Cannot determine the fully qualified hostname of this PAM

PAM-CMN-2818 = Cannot register PAM into {0}  
PAM-CMN-2819 = Cannot assign a partition for {0}  
PAM-CMN-2831 = PAM is currently provisioned to use OpenSSL and the password is not cached!  
PAM-CMN-2832 = PAM is re-encrypting the DB. Please try again later.  
PAM-CMN-2834 = No storage element for PAM on {0}. Please try again.  
PAM-CMN-2837 = PAM is currently provisioned to use WolfSSL and the password is not cached!  
PAM-CMN-2838 = Success, you must reboot PAM for this change to take effect.

PAM-CMN-3016 = Access denied.  
PAM-CMN-3017 = Too many authentication failures for {0}  
PAM-CMN-3018 = Cannot change user when server not running as root.  
PAM-CMN-3022 = bad service request {0}  
PAM-CMN-3026 = Change of username or service not allowed: ({0},{1}) -> ({2},{3})  
PAM-CMN-3075 = Timeout, your session not responding.  
PAM-CMN-3076 = wait: {0}  
PAM-CMN-3077 = Command terminated on signal {0}.  
PAM-CMN-3078 = wait returned status {0}  
PAM-CMN-3079 = server\_input\_channel\_req: unknown channel %d  
PAM-CMN-3081 = socket: {0}  
PAM-CMN-3082 = bind: {0}  
PAM-CMN-3083 = listen: {0}  
PAM-CMN-3084 = Session.c: Only subsystem SFTP allowed  
PAM-CMN-3085 = Could not create pipes: {0}  
PAM-CMN-3086 = Could not create socket pairs: {0}  
PAM-CMN-3087 = fork failed: {0}  
PAM-CMN-3088 = dup #1 failed: {0}  
PAM-CMN-3089 = dup #2 failed: {0}  
PAM-CMN-3090 = Protocol error: you already have a pty.  
PAM-CMN-3102 = Your ssh version is too old and is no longer supported. Please install a newer version.  
PAM-CMN-3103 = Connection to remote server failed  
PAM-CMN-3104 = Client disconnected  
PAM-CMN-3106 = IP Spoofing check bytes do not match.

PAM-CMN-3142 = DNS Error resolving IP

PAM-CMN-3154 = AuthBroker: Some general exception occurred  
PAM-CMN-3155 = Unknown Exception caught in AuthDaemon. Shutting down engine. Exiting  
PAM-CMN-3156 = ServiceThread: Caught exception unbeknownst to anyone. Eating up this exception  
PAM-CMN-3157 = This Authentication Type is not supported by the PAM GK yet.  
PAM-CMN-3158 = No server session id found in the accesschallengeretort message.  
PAM-CMN-3159 = The Protocol demands that userId must be blank while responding to a challenge but I found this lingering userid: {0}  
PAM-CMN-3160 = No GKAuthenticationAgent found for the given session id in the accesschallengeretort message.  
PAM-CMN-3161 = Only challenge response expected at this point.  
PAM-CMN-3162 = Different Session id in the challenge retort  
PAM-CMN-3163 = Your password will expire in {0} day(s)  
PAM-CMN-3164 = Your account will expire in {0} day(s)

PAM-CMN-3234 = The HSM is not functioning properly with PKCS11 result: {0}, {1}  
PAM-CMN-3235 = OpenSSL JNI library result: {0}, {1}

PAM-CMN-3240 = Submit  
PAM-CMN-3241 = Submit Response  
PAM-CMN-3242 = Your new PIN has been set into the system. Please wait for the tokencode to change, then authenticate again with your complete passcode now.

PAM-CMN-3243 = To continue you must enter a new PIN. Enter a new PIN of {0} alphanumeric characters:  
PAM-CMN-3244 = To continue you must enter a new PIN. Enter a new PIN between {0} and {1} alphanumeric characters:  
PAM-CMN-3245 = To continue you must enter a new PIN. Enter a new PIN of {0} digits:  
PAM-CMN-3246 = To continue you must enter a new PIN. Enter a new PIN between {0} and {1} digits:  
  
PAM-CMN-3250 = Applets signed successfully with {0} and domain(s) {1}.  
PAM-CMN-3251 = The Java KeyStore file doesn't exist at {0}. Aborting signature.  
  
PAM-CMN-3274 = No response from Password Authority.  
PAM-CMN-3275 = {0} does not exist or is empty.  
PAM-CMN-3276 = {0} is not readable.  
PAM-CMN-3277 = {0} is not a regular file.  
  
PAM-CMN-3300 = Reauthentication request failed for user {0}.  
PAM-CMN-3301 = Session id was not in proper format. Cannot apply reauthentication mitigation for the session  
  
PAM-CMN-3319 = Exceeded the maximum number of allowed violations. Session will be terminated.  
PAM-CMN-3320 = User name exceeds maximum length of {0}.  
PAM-CMN-3321 = User group name exceeds maximum length of {0}.  
PAM-CMN-3322 = Device name exceeds maximum length of {0}.  
PAM-CMN-3323 = Device group name exceeds maximum length of {0}.  
PAM-CMN-3324 = User's first name exceeds maximum length of {0}.  
PAM-CMN-3325 = User's last name exceeds maximum length of {0}.  
PAM-CMN-3326 = Invalid numeric data. Device Group id must be a positive integer.  
PAM-CMN-3327 = The database has been loaded successfully from {0}.  
  
PAM-CMN-3331 = Attempt was made to update command filter metrics on a session with no matching command filter configuration  
  
PAM-CMN-3356 = Remote CA PAM Debugging Services is ON.  
PAM-CMN-3357 = MySQL Enterprise Monitor is installed. This should be used for debugging only.  
PAM-CMN-3358 = This appliance is in maintenance mode.  
PAM-CMN-3359 = This appliance's local PA is inactive.  
PAM-CMN-3360 = This secondary site member is deactivated.  
PAM-CMN-3361 = This secondary site member's access db is OOS with the primary site.  
PAM-CMN-3363 = Filter "{0}" not updated. List type for this entry does not match first entry type of "{1}".  
PAM-CMN-3364 = Getting all filters to export ...  
PAM-CMN-3365 = Invalid task information for device, see log for details.  
  
PAM-CMN-3366 = Auto-login initiated with target account Name : {0} and target account Id : {1} and ticket ID : {2}.  
PAM-CMN-4058 = Invalid characters found in name of file to be uploaded. File name can only have alphanumeric characters plus dash, underscore and period. Please change the file name.  
PAM-CMN-4059 = Time server {0} cannot be resolved to IP address.  
PAM-CMN-5400 = Failed to save NIM credentials on member {0}. Unable to establish a connection to the CA PAM appliance.  
PAM-CMN-5401 = Saving NIM credentials on all cluster members failed for {0}/{1} members: {2}.  
PAM-CMN-5402 = NIM credentials saved on all cluster members.  
PAM-CMN-5403 = Saving NIM credentials failed.  
PAM-CMN-5404 = NIM credentials saved. PAM-CMN-5406 = PKI authentication failed. Contact your system administrator to check the session log for errors.  
PAM-CM-6003: Inactive users are deactivated on-demand.  
PAM-CM-6004: Deactivation reminder notification emails have been sent on-demand.  
PAM-CM-6005: Failed to deactivate inactive users on-demand.  
PAM-CM-6006: Failed to send deactivation reminder notification emails on-demand.



## Transparent Login Messages

PAM-TLGN-0060: CA PAM user who is transparently logged into RDP Application <ApplicationName> to <WindowsTitle> window as <Username> user, at <Device> device.

**ApplicationName** – The name of the RDP application defined in Privileged Access Manager

**WindowsTitle** – The title of the window that the end-user used to log in

**Username** – The name of the target account that was used

**Device** – The credential source

## PAM-CS: Cluster Status Messages

PAM-CS-0001 = Database Cluster Replication Status from PAM Instance {0}

PAM-CS-0002 = The following primary site cluster members are no longer participating in database replication: {0}

PAM-CS-0003 = Failed retrieving list of unavailable cluster replication members: {0}

PAM-CS-0004 = ONLINE

PAM-CS-0005 = OFFLINE

PAM-CS-0006 = RECOVERING

PAM-CS-0007 = UNREACHABLE

PAM-CS-0008 = ERROR

PAM-CS-0009 = MISSING

PAM-CS-0010 = The following primary site cluster members are no longer participating in database replication: {0}

PAM-CS-0011 = Database cluster replication status: {0}.

PAM-CS-0012 = Failed refreshing list of unavailable cluster replication members

PAM-CS-0013 = The database is out of sync with the primary site for the following secondary site members: {0}

PAM-CS-0014 = CA PAM Cluster Failure: Please check the status of each member in the primary site

PAM-CS-0015 = CA PAM instance {0} lost its connection to other members of the primary site, and has limited functionality. Please check the availability of other primary site members to ensure that they are online and reachable. Next, check their status by visiting their respective URLs: {1}. If you cannot access other members, visit https://{2} to repair the cluster.

PAM-CS-0016 = CA PAM Cluster is recovering

PAM-CS-0017 = CA PAM instance {0} can now communicate with all members of the cluster's primary site. To recover from a previous failure, we are rebooting the CA PAM instance.

PAM-CS-0018 = CA PAM Cluster is recovering the primary site

PAM-CS-0019 = We are rebooting all the members in the primary site of CA PAM Cluster to try to recover it from a previous failure.

PAM-CS-0020 = PAM appliance attempted to perform cluster operation on {0}, but is not part of its cluster list.

PAM-CS-0021 = The database is back online and participating in replication for the following primary site cluster members: {0}

PAM-CS-0022 = If the database is out of sync with the primary site for {0} more minutes, deactivation occurs.

PAM-CS-0023 = The database is back in sync with the primary site for the following secondary site members: {0}

## PAM-IMP: Import and Export Constants

PAM-IMP-0001="Export"

PAM-IMP-0002="Import"

PAM-IMP-0003="Devices"

PAM-IMP-0004="Users"

PAM-IMP-0005="Services"  
PAM-IMP-0006="Transparent Login Configs"  
PAM-IMP-0007="Custom Roles"  
PAM-IMP-0008="Policy"  
PAM-IMP-0009="Socket Filter Lists"  
PAM-IMP-0010="Command Filter Lists"  
PAM-IMP-0011="SAML 2.0 SP Metadata"

## PAM-LDAP: LDAP Importer Messages

PAM-LDAP-0000 = Error updating member {0} {1}  
PAM-LDAP-0001 = The CA PAM cluster is not synchronized. LDAP update will not be attempted.  
PAM-LDAP-0002 = The CA PAM cluster is not synchronized. LDAP operation will not be attempted.  
PAM-LDAP-0003 = All servers to LDAP domain {0} are down. LDAP sync for group {1} will not be attempted.  
PAM-LDAP-0004 = An exception ( {0} ) occurred while processing LDAP group {1}. LDAP sync for this group will be aborted.  
PAM-LDAP-0005 = Device {0} deleted from LDAP group {1} but is a member of other registered LDAP groups.  
PAM-LDAP-0006 = User {0} deleted from LDAP group {1} but is a member of other registered LDAP groups.  
PAM-LDAP-0007 = Updating LDAP Group {0} failed. Connection to all configured LDAP servers failed. {1} New Users, {2} Updated Users, {3} Deleted Users, {4} Failed New Users, {5} Failed Updated Users, {6} Failed Deleted Users, {7} Users Retrieved From LDAP Directory Server  
PAM-LDAP-0008 = Updating LDAP Group {0} failed. Connection to all configured LDAP servers failed. {1} New Devices, {2} Updated Devices, {3} Deleted Devices, {4} Failed New Devices, {5} Failed Updated Devices, {6} Failed Deleted Devices, {7} Devices Retrieved From LDAP Directory Server  
PAM-LDAP-0009 = LDAP Group {0} updated. {1} New Users, {2} Updated Users, {3} Deleted Users, {4} Failed New Users, {5} Failed Updated Users, {6} Failed Deleted Users, {7} Users Retrieved From LDAP Directory Server  
PAM-LDAP-0010 = LDAP Group {0} updated. {1} New Devices, {2} Updated Devices, {3} Deleted Devices, {4} Failed New Devices, {5} Failed Updated Devices, {6} Failed Deleted Devices, {7} Devices Retrieved From LDAP Directory Server  
PAM-LDAP-0011 = Error occurred while replicating LDAP changes across the cluster  
PAM-LDAP-0012 = Exception occurred while replicating LDAP changes across the cluster  
PAM-LDAP-0013 = Error occurred while removing deleted import data {0}{1}{2}  
PAM-LDAP-0014 = Error occurred while importing member {0}{1}{2}  
PAM-LDAP-0015 = Warning adding device {0} {1}  
PAM-LDAP-0016 = Error adding device {0} {1}  
PAM-LDAP-0017 = Warning adding user {0} {1}  
PAM-LDAP-0018 = Error adding user {0} {1}  
PAM-LDAP-0019 = Error occurred while removing deleted import data {0}{1}{2}  
PAM-LDAP-0020 = SQL error occurred importing ldap member {0}{1}{2}  
PAM-LDAP-0021 = There was a problem importing member {0}{1}{2}  
PAM-LDAP-0022 = User {0} was moved to: {1}  
PAM-LDAP-0023 = Exception occurred while trying to retrieve the members of group {0} via the primary group token {1}  
PAM-LDAP-0024 = Search or processing of group {0} failed with exception {1}  
PAM-LDAP-0025 = LDAP group {0} not found in domain.  
PAM-LDAP-0026 = Group {0} was moved to {1}  
PAM-LDAP-0027 = Group {0} was deleted on LDAP server  
PAM-LDAP-0028 = Search of group {0} failed with exception {1}  
PAM-LDAP-0029 = Search of OU {0} failed with exception {1}  
PAM-LDAP-0030 = Exception occurred while retrieving the members of group {0} Exception: {1}  
PAM-LDAP-0031 = Retrieving attributes of member {0} failed with exception {1}

PAM-LDAP-0032 = LDAP member {0} not found in domain {1}  
 PAM-LDAP-0033 = CA PAM is unable to determine the domain that owns SID {0}. Is the domain configured with CA PAM?  
 Unable to import member from group {1}  
 PAM-LDAP-0034 = The object class of the member {0} is unrecognized: {1}  
 PAM-LDAP-0035 = Binding to domain {0} failed. Invalid LDAP admin password configured.  
 PAM-LDAP-0036 = Unable to connect to domain {0}. All configured LDAP servers are down.  
 PAM-LDAP-0037 = Exception occurred while processing a search on entity {0}: {1}  
 PAM-LDAP-0038 = Connection to LDAP {0} failed. Failing over to the next configured server for the domain.

## PAM-MGC: Management Console Messages

PAM-MGC-0001 = Failed to determine cluster structure. Service cannot start. Name:{0}  
 PAM-MGC-0002 = Failed to determine any node IP addresses. Service cannot start. Name:{0}  
 PAM-MGC-0003 = Local addresses count:{0}  
 PAM-MGC-0004 = Failed to determine REST request path. Request:{0}, Message:{1}  
 PAM-MGC-0005 = Recognized REST request path. Request:{0}  
 PAM-MGC-0006 = Failed to recognize REST request path. Request:{0}  
 PAM-MGC-0007 = Management Console servlet status:{0}, Servlet:{1}, Active:{2}, Mode:{3}, Message:{4}  
 PAM-MGC-0008 = Failed to determine local IP address. Message:{0}  
 PAM-MGC-0009 = Failed to retrieve cluster structure. Message:{0}  
 PAM-MGC-0010 = Failed to read cluster structure data. Message:{0}  
 PAM-MGC-0011 = Failed to check Management Console license.  
 PAM-MGC-0012 = Failed to read cluster structure object. Message:{0}  
 PAM-MGC-0013 = Failed to obtain public addresses from cluster structure. Message:{0}  
 PAM-MGC-0014 = Failed to read cluster info data. Message:{0}  
 PAM-MGC-0015 = Failed to read cluster data. Message:{0}  
 PAM-MGC-0016 = Failed to read system Info data. Message:{0}  
 PAM-MGC-0017 = Cluster member added. IP:{0}  
 PAM-MGC-0018 = Cluster Member removed. IP:{0}  
 PAM-MGC-0019 = Could not create target download directory. Path:{0}  
 PAM-MGC-0020 = Could not create staged patch directory. Path:{0}  
 PAM-MGC-0021 = Failed to download entire patch file. ID:{0}, Downloaded Size:{1}, Expected size:{2}  
 PAM-MGC-0022 = Failed to download the patch without errors. ID:{0}, Downloaded SHA1:{1}, Expected SHA1:{2}  
 PAM-MGC-0023 = Patch download completed. ID:{0}, File:{1}, Size:{2}  
 PAM-MGC-0024 = Failed to move downloaded patch to target dir. ID:{0}, From:{1}, To:{2}  
 PAM-MGC-0025 = Failed to verify existing patch file match. File:{0}, Message:{1}  
 PAM-MGC-0026 = Failed to decrypt target API password from configuration. Message:{0}  
 PAM-MGC-0027 = Could not obtain Management Console session ID. Task was aborted -- will retry. Task Name:{0}  
 PAM-MGC-0028 = Incomplete task prerequisites. Task was aborted -- will retry. Task Name:{0}  
 PAM-MGC-0029 = Task failed. Task:{0}, Message:{1}  
 PAM-MGC-0030 = Could not construct staged inventory lookup map.  
 PAM-MGC-0031 = Could not construct appliance lookup map.  
 PAM-MGC-0032 = Failed to submit status request to Management Console. Status:{0}, Reason:{1}, URI:{2}  
 PAM-MGC-0033 = Failed to submit status request data. URI:{0}  
 PAM-MGC-0034 = Unknown section type in Management Console status request processing. Type:{0}  
 PAM-MGC-0035 = Scheduling purge for a staged patch. ID:{0}  
 PAM-MGC-0036 = Processing status response. Version:{0}  
 PAM-MGC-0037 = Unimplemented staging task request. Request:{0}, File:{1}  
 PAM-MGC-0038 = Failed to submit ACK for a previously received file. Downloading again. File:{0}, Inventory:{1}  
 PAM-MGC-0039 = Failed to submit ACK for symlink staged file. File:{0}, To:{1}, Inventory:{2}  
 PAM-MGC-0040 = Failed to make symlink to inventory file. From:{0}, To:{1}, Inventory:{2}, Message:{3}  
 PAM-MGC-0041 = Failed to start patch download. Task ID:{0}, Status:{1}, Message:{2}, URI:{3}

PAM-MGC-0042 = Failed to submit ACK for downloaded staged file. File:{0}, Inventory:{1}  
PAM-MGC-0043 = Failed to download patch file. Task ID:{0}, Message:{1}  
PAM-MGC-0044 = Failed to delete patch file. Task ID:{0}, File:{1}  
PAM-MGC-0045 = Failed to submit ACK for received patch download. File:{0}, Size:{1}, Task ID:{2}, Status:{3}, Message:{4}  
PAM-MGC-0046 = Could not extract download tag information. ID:{0}, Tag:{1}, Message:{2}  
PAM-MGC-0047 = Failed to read the inventory of managed patches.  
PAM-MGC-0048 = Managed patch directory does not exist. Directory:{0}  
PAM-MGC-0049 = Could not delete managed inventory file. File:{0}, Message:{1}  
PAM-MGC-0050 = Could not find the aggregator IP address. MC Reporting task was aborted -- will retry.  
PAM-MGC-0051 = Appliance has not yet registered with the aggregator node. Will attempt.  
PAM-MGC-0052 = Failed to read the appliance registration record. Hardware ID:{0}, Message:{1}  
PAM-MGC-0053 = Failed to read the appliance record. Hardware ID:{0}, Message:{1}  
PAM-MGC-0054 = Failed to submit appliance update request to the aggregator node. Status:{0}, Reason:{1}, Aggregator IP:{2}, Hardware ID:{3}  
PAM-MGC-0055 = Failed to update the appliance with the aggregator node. Aggregator:{0}, Hardware ID:{1}, Message:{2}  
PAM-MGC-0056 = Failed to submit appliance registration request to the aggregator node. Status:{0}, Reason:{1}, Aggregator:{2}, Hardware ID:{3}  
PAM-MGC-0057 = Failed to auto-register the appliance with the aggregator node. Aggregator:{0}, Hardware ID:{1}, Message:{2}  
PAM-MGC-0058 = Failed to read the inventory of staged patches. Message:{0}  
PAM-MGC-0059 = Could not delete file from staging directory. Path:{0}, Message:{1}  
PAM-MGC-0060 = Could not delete patch file link from upgrade-stage dir. Path:{0}, Message:{1}  
PAM-MGC-0061 = Patch file not yet available in staged inventory. File:{0}  
PAM-MGC-0062 = Failed to make symlink for upgrade file. From:{0}, To:{1}, Message:{2}  
PAM-MGC-0063 = Failed to read ACK record from database. Item:{0}, Hardware ID:{1}, Patch ID:{2}, Message:{3}  
PAM-MGC-0064 = Unexpected response to staging action report from the aggregator node. Status:{0}, Reason:{1}, Aggregator:{2}, Hardware ID:{3}  
PAM-MGC-0065 = Failed to send staging action request to the aggregator node. Aggregator:{0}, Hardware ID:{1}, Patch ID:{2}, Action:{3}, Message:{4}  
PAM-MGC-0066 = Could not delete staged inventory file. File:{0}, Message:{1}  
PAM-MGC-0067 = Failed to download information. Message:{0}, Patch ID:{1}, URI:{2}, Message:{3}  
PAM-MGC-0068 = Starting PAMMC servlet task. Task type:{0}  
PAM-MGC-0069 = Ended Management Console servlet task. Task type:{0}  
PAM-MGC-0070 = Management Console servlet task failed. Task type:{0}, Message:{1}  
PAM-MGC-0071 = Could not read license file. Message:{0}  
PAM-MGC-0072 = Unknown command in activate. Name:{0}  
PAM-MGC-0074 = Rejected request from remote address. IP Address:{0}  
PAM-MGC-0075 = Serviced an HTTP request. Action={0}, Status:{1}  
PAM-MGC-0076 = Management Console servlet task failed to initialize. Task type:{0}  
PAM-MGC-0077 = Management Console servlet task timers were stopped. Enabled-Check task running status:{0}  
PAM-MGC-0079 = Failed to stop the Management Console integration servlet. Response code:{0}  
PAM-MGC-0082 = Connected successfully to the Management Console. Host:{0}  
PAM-MGC-0083 = Could not connect to the Management Console. Host:{0}  
PAM-MGC-0084 = Connected successfully to the Management Console integration API. Host:{0}, Message:{1}  
PAM-MGC-0085 = Could not connect to the Management Console integration API. Service is temporarily unavailable. Host:{0}  
PAM-MGC-0086 = Management Console integration API test failed. Host:{0}, Status:{1}  
PAM-MGC-0087 = Failed to retrieve aggregator credentials for Reporting API test.  
PAM-MGC-0088 = Connected successfully to the Management Console reporting API. Host:{0}, Message:{1}  
PAM-MGC-0089 = Could not connect to the Management Console Reporting API. Service is temporarily unavailable. Host:{0}

PAM-MGC-0090 = Management Console reporting API test failed. Host:{0}, Status:{1}  
PAM-MGC-0091 = Failed to stop the Management Console service servlet. Response Code:{0}  
PAM-MGC-0093 = Console appliance created: Location:{0}, Name:{1}  
PAM-MGC-0094 = This member is not registered for Management Console reporting.  
PAM-MGC-0095 = This member is already registered for Management Console reporting.  
PAM-MGC-0096 = Failed to perform local appliance lookup test. Message:{0}  
PAM-MGC-0097 = Console appliance updated: Location:{0}, Name:{1}  
PAM-MGC-0098 = Console appliance deleted: Location:{0}, Name:{1}  
PAM-MGC-0104 = Console cluster created. Name:{0}, Active:{1}  
PAM-MGC-0106 = Console cluster name is not defined.  
PAM-MGC-0108 = Console cluster updated. Name:{0}, Active:{1}  
PAM-MGC-0109 = Device host for cluster is missing. Host ID:{0}, Cluster Name:{1}  
PAM-MGC-0111 = Error processing status report. Message:{0}  
PAM-MGC-0112 = Unknown request protocol. Version:{0}  
PAM-MGC-0113 = Unrecognized status section in FullStatus. Section ID:{0}, Cluster:{1}  
PAM-MGC-0114 = Unrecognized status value in staging task. Value:{0}  
PAM-MGC-0115 = Unknown response protocol. Version:{0}  
PAM-MGC-0116 = Unsupported request/response protocol pair: Request:{0}, Response:{1}  
PAM-MGC-0117 = Console inventory patch ID is not defined.  
PAM-MGC-0118 = Upload file is not available. Name:{0}  
PAM-MGC-0119 = Unimplemented staging task ACK command. Command:{0}, Task:{1}  
PAM-MGC-0121 = Patch staging task created. Cluster:{0}, Patch:{1}, Action:{2}  
PAM-MGC-0122 = Recall action skipped for staging task. Task ID:{0}, Task state:{1}  
PAM-MGC-0123 = Cluster staging task updated. Cluster:{0}, Patch:{1}, Action:{2}, Status:{3}  
PAM-MGC-0124 = Error occurred while deleting staging tasks for Cluster. Cluster ID:{0}  
PAM-MGC-0125 = Deleted staging task. Task ID:{0}  
PAM-MGC-0126 = Error occurred while deleting staging task. Task ID:{0}  
PAM-MGC-0127 = Unknown servlet action request. Name:{0}  
PAM-MGC-0128 = Error processing request. Message:{0}  
PAM-MGC-0129 = Processing patch upload file. File:{0}, Directory:{1}  
PAM-MGC-0130 = Completed processing patch upload file. File:{0}, Object:{1}  
PAM-MGC-0131 = Error decrypting patch file. BIN file:{0}, Message:{1}  
PAM-MGC-0132 = Error loading patch metadata file. INF file:{0}, Message:{1}  
PAM-MGC-0133 = Error examining flags in the patch BIN file. File:{0}, Message:{1}  
PAM-MGC-0134 = Error decompressing the uploaded file. File:{0}, Message:{1}  
PAM-MGC-0135 = Error calculating file SHA1 hash. File:{0}, Message:{1}  
PAM-MGC-0136 = Servlet stopped.  
PAM-MGC-0137 = Patch download from Management Console succeeded. File:{0}  
PAM-MGC-0138 = Patch download from Management Console failed. File:{0}  
PAM-MGC-0139 = Call to Credential Manager failed. Message:{0}  
PAM-MGC-0140 = Failed to get upgrade history for patch. Patch ID:{0}, Message:{1}  
PAM-MGC-0141 = Could not obtain Management Console integration servlet configuration.  
PAM-MGC-0142 = Management Console integration servlet startup is not required. Servlet is disabled.  
PAM-MGC-0143 = Could not obtain local node hardware ID.  
PAM-MGC-0144 = Servlet started.  
PAM-MGC-0145 = Could not perform integration test. Test:{0}, Message:{1}  
PAM-MGC-0146 = Could not call Management Console integration servlet. Test:{0}, Message:{1}  
PAM-MGC-0147 = Management Console integration module was activated.  
PAM-MGC-0148 = Management Console integration module was deactivated.  
PAM-MGC-0149 = Could not activate Management Console integration module.  
PAM-MGC-0150 = Could not deactivate Management Console integration module.  
PAM-MGC-0151 = Unknown protocol. Version:{0}  
PAM-MGC-0152 = Unknown submitted status object. Message:{0}



PAM-MGC-0153 = Console cluster deleted. Name:{0}  
PAM-MGC-0154 = Console inventory item created. Patch ID:{0}  
PAM-MGC-0155 = Console inventory item updated. Patch ID:{0}, Archive:{1}  
PAM-MGC-0156 = Console inventory item deleted. Patch ID:{0}  
PAM-MGC-0157 = Patch file name is not defined.  
PAM-MGC-0158 = Failed to move patch file to inventory. Location:{0}  
PAM-MGC-0159 = Console licenses created. Cluster name:{0}  
PAM-MGC-0160 = Console licenses updated. Cluster name:{0}  
PAM-MGC-0161 = Console licenses deleted. Cluster name:{0}  
PAM-MGC-0162 = Console licenses ID is not defined.  
PAM-MGC-0163 = Console cluster ID is not defined.  
PAM-MGC-0164 = Unknown archive file type. Name:{0}  
PAM-MGC-0165 = File upload succeeded. Name:{0}  
PAM-MGC-0166 = Could not call Management Console service servlet. Test:{0}, Message:{1}  
PAM-MGC-0167 = Management Console service module was activated.  
PAM-MGC-0168 = Management Console service module was deactivated.  
PAM-MGC-0169 = Could not activate Management Console service module.  
PAM-MGC-0170 = Could not deactivate Management Console service module.  
PAM-MGC-0171 = Device for Management Console cluster. Cluster:{0}, Device ID:{1}, Message:{2}  
PAM-MGC-0172 = Failed to create device for cluster. Name:{0}  
PAM-MGC-0173 = Failed to create application for cluster. Cluster name: {0}  
PAM-MGC-0174 = Target account for cluster is missing. Account ID:{0}, Cluster name:{1}  
PAM-MGC-0175 = Device/Host for cluster is missing. Host ID:{0}, Cluster name:{1}  
PAM-MGC-0176 = Could not obtain status processing lock. Cluster cookie:{0}  
PAM-MGC-0177 = This cluster is already managed by the Management Console.  
PAM-MGC-0178 = This cluster is not managed by the Management Console.  
PAM-MGC-0179 = Requested task to retry does not exist. ID:{0}  
PAM-MGC-0180 = Failed to parse staging event action hint. Value:{0}  
PAM-MGC-0181 = Could not mark the successful transfer completion for a Staging Task. Task ID:{0}, Message:{1}  
PAM-MGC-0182 = Could not obtain Management Console service servlet configuration.  
PAM-MGC-0183 = Could not obtain Management Console service bandwidth limiter configuration.  
PAM-MGC-0184 = Management Console Service servlet startup is not required. Servlet is disabled.  
PAM-MGC-0185 = Patch was recalled from staging inventory. File:{0}  
PAM-MGC-0186 = Staged patch was deleted. File:{0}  
PAM-MGC-0187 = Staging inventory item created. Patch ID:{0}  
PAM-MGC-0188 = Staging inventory item updated. Patch ID:{0}, Archive:{1}  
PAM-MGC-0189 = Staging inventory item deleted. Patch ID:{0}  
PAM-MGC-0190 = Upgrade patch was staged. File:{0}  
PAM-MGC-0191 = Upgrade patch was removed. File:{0}  
PAM-MGC-0192 = Error extracting file checksum hash. File:{0}  
PAM-MGC-0193 = Server protocol switched after error from version {3} to {4}. Status:{0}, Reason:{1}, URI:{2}

## PAM-PAMSC: PAM SC Device Matching Messages

- PAM-PAMSC-0073: Match operation initiated to match Server Control host <hostname> to PAM device <Device name>.
- PAM-PAMSC-0074: Unmatch operation initiated to unmatch Server Control host <hostname> from PAM device <Device name>.
- PAM-PAMSC-0075: Device Matching Configuration updated. Enabled: <true|false> PAM device name match: <EXACT|PARTIAL|DISABLED> PAM device address match: <EXACT|PARTIAL|DISABLED>; Automatic duplicate device matching: <true|false>.
- PAM-PAMSC-0076: Duplicate device matching run initiated manually.
- PAM-PAMSC-0077: Duplicate device matching run completed.
- PAM-PAMSC-0078: Successfully matched Server Control host <hostname> to PAM device <Device name>.

## PAM-PRX: Proxy Messages

PAM-PRX-0000 = X11 forwarded as {0}  
 PAM-PRX-0001 = Launched X11 application  
 PAM-PRX-0002 = Enabled X11 forwarding as {0}  
 PAM-PRX-0003 = Executed {0} as {1}  
 PAM-PRX-0004 = gatekeeper[{0}]: telnetproxy, fail to activate SFA, SFA enforced, service discarded  
 PAM-PRX-0005 = gatekeeper[{0}]: telnetproxy, cannot get address info  
 PAM-PRX-0006 = gatekeeper[{0}]: telnetproxy, fail to connect to target device  
 PAM-PRX-0007 = gatekeeper[{0}]: sshproxy, fail to connect to target device  
 PAM-PRX-0008 = gatekeeper[{0}]: sshproxy, fail to activate SFA, SFA enforced, service discarded  
 PAM-PRX-0009 = File transfers are not permitted via SSH TCP service  
 PAM-PRX-0010 = SSH TCP service unknown sub-system  
 PAM-PRX-0011 = This connection cleaned up due to a problem with the recording storage.  
 PAM-PRX-0012 = Launched X11 application "{0}"  
 PAM-PRX-0013 = File transfers are not permitted via SSH TCP service.  
 PAM-PRX-0014 = X11 forwarding services are not permitted  
 PAM-PRX-0015 = Services are not permitted via SSH TCP service.  
 PAM-PRX-0016 = Executed "{0}" using transparent login as {1}  
 PAM-PRX-0017 = Session disconnected due to a problem with session recording  
 PAM-PRX-0018 = Auto-login using username {0}  
 PAM-PRX-0019 = no authentication methods enabled  
 PAM-PRX-0020 = Connection from {0} with IP options: {1}  
 PAM-PRX-0021 = Received data for nonexistent channel {0}.  
 PAM-PRX-0022 = Received extended\_data for bad channel {0}.  
 PAM-PRX-0023 = Received extended\_data after EOF on channel {0}.  
 PAM-PRX-0024 = Received ieof for nonexistent channel {0}.  
 PAM-PRX-0025 = Received close for nonexistent channel {0}.  
 PAM-PRX-0026 = Received oclose for nonexistent channel {0}.  
 PAM-PRX-0027 = Received close confirmation for out-of-range channel {0}.  
 PAM-PRX-0028 = Received close confirmation for non-closed channel {0} (type {1}).  
 PAM-PRX-0029 = Received open confirmation for non-opening channel {0}.  
 PAM-PRX-0030 = Received open failure for non-opening channel {0}.  
 PAM-PRX-0031 = getaddrinfo: fatal error  
 PAM-PRX-0032 = Protocol error for port forward request: received packet type {0}.  
 PAM-PRX-0033 = Requested forwarding of port {0} but user is not root.  
 PAM-PRX-0034 = Dynamic forwarding denied  
 PAM-PRX-0035 = protocol error: rcvd type {0}  
 PAM-PRX-0036 = bad server public DH value

PAM-PRX-0037 = Protocol error: no matching DH grp found  
 PAM-PRX-0038 = Protocol error: expected packet type {0}, got {1}  
 PAM-PRX-0039 = SSH1, Bad packet length {0}.  
 PAM-PRX-0040 = crc32 compensation attack: network attack detected  
 PAM-PRX-0041 = packet\_read\_poll1: len {0} != buffer\_len {1}.  
 PAM-PRX-0042 = Corrupted check bytes on input.  
 PAM-PRX-0043 = SSH2, Bad packet length {0}.  
 PAM-PRX-0044 = Corrupted MAC on input.  
 PAM-PRX-0045 = Corrupted padlen {0} on input.  
 PAM-PRX-0046 = Packet corrupt  
 PAM-PRX-0047 = Bad packet length {0}.  
 PAM-PRX-0048 = deattack denial of service detected  
 PAM-PRX-0049 = Invalid ssh1 packet type: {0}  
 PAM-PRX-0050 = Invalid ssh2 packet type: {0}  
 PAM-PRX-0051 = Packet integrity error.  
 PAM-PRX-0052 = Possible attack: attempt to open a session after additional sessions disabled  
 PAM-PRX-0053 = command execution failed  
 PAM-PRX-0054 = shell execution failed  
 PAM-PRX-0055 = Protocol error waiting for compression response.  
 PAM-PRX-0056 = Protocol error waiting for pty request response.  
 PAM-PRX-0057 = Protocol error waiting for X11 forwarding  
 PAM-PRX-0058 = Protocol error during RSA authentication: {0}  
 PAM-PRX-0059 = Protocol error waiting RSA auth response: {0}  
 PAM-PRX-0060 = respond\_to\_rsa\_challenge: rsa\_private\_decrypt failed  
 PAM-PRX-0061 = respond\_to\_rsa\_challenge: bad challenge length {0}  
 PAM-PRX-0062 = Protocol error: got {0} in response to {1}  
 PAM-PRX-0063 = Your password will expire in {0} day(s)  
 PAM-PRX-0064 = Your account will expire in {0} day(s)  
 PAM-PRX-0065 = Could not grab keyboard or mouse. A malicious client may be eavesdropping on your session.  
 PAM-PRX-0066 = Enter your OpenSSH passphrase:  
 PAM-PRX-0067 = Could not grab {0}. A malicious client may be eavesdropping on your session.  
 PAM-PRX-0068 = Enter {0}@{1}'s old password:  
 PAM-PRX-0069 = Enter {0}@{1}'s new password:  
 PAM-PRX-0070 = Retype {0}@{1}'s new password:  
 PAM-PRX-0071 = Fail to activate SFA, SFA enforced, service discarded  
 PAM-PRX-0072 = Too many authentication failures for {0} {1} from {2} port {3} {4}  
 PAM-PRX-0073 = Authentication rejected for uid {0}.  
 PAM-PRX-0074 = gatekeeper[{0}]: {1}, failed to connect to target device

## PAM-SP: SailPoint Messages

PAM-SP-0001 = Exported CA-PAM Roles into SailPoint: {0} roles added, {1} roles deleted.  
 PAM-SP-0002 = Exported CA-PAM User Groups into SailPoint: {0} groups added, {1} groups deleted.  
 PAM-SP-0003 = Exported CA-PAM Users into SailPoint: {0} users added, {1} users modified, {2} users deleted.  
 PAM-SP-0004 = Created SailPoint Account {0}.  
 PAM-SP-0005 = Updated SailPoint Account {0}.  
 PAM-SP-0006 = Deleted SailPoint Account {0}.  
 PAM-SP-0007 = Created SailPoint User Group {0}.  
 PAM-SP-0008 = Updated SailPoint User Group {0}.



PAM-SP-0009 = Deleted SailPoint User Group {0}.  
 PAM-SP-0010 = Created SailPoint Role {0}.  
 PAM-SP-0011 = Updated SailPoint Role {0}.  
 PAM-SP-0012 = Deleted SailPoint Role {0}.  
 PAM-SP-0013 = Imported user {0} from SailPoint.  
 PAM-SP-0014 = Imported User Group {0} from SailPoint for user {1}.  
 PAM-SP-0015 = Imported role {0} from SailPoint for user {1}.  
 PAM-SP-0016 = Deleted user {0} that was deleted from SailPoint.  
 PAM-SP-0017 = Removed User Group {0} that was deleted from SailPoint for user {1}.  
 PAM-SP-0018 = Removed role {0} that was deleted from SailPoint for user {1}.  
 PAM-SP-0019 = Import of SailPoint data successful: {0} records processed.  
 PAM-SP-0020 = Disabled SailPoint Account {0}.  
 PAM-SP-0021 = Enabled SailPoint Account {0}.  
 PAM-CM-2104 = Updated SailPoint configuration

## PAM-SPFD: Secure Port Forwarding Daemon Messages

PAM-SPFD-0001 = CA PAM[{0}]: Connections to local addresses not permitted.  
 PAM-SPFD-0002 = Connection to '{0}' has been blocked by VMware NSX Security Policy.  
 PAM-SPFD-0003 = CA PAM[{0}]: Mismatched version of Monitoring agent is running on target device.  
 PAM-SPFD-0004 = CA PAM[{0}]: Monitoring agent is not running on device.  
 PAM-SPFD-0005 = CA PAM[{0}]: Login is not allowed if Monitoring agent is unreachable.  
 PAM-SPFD-0006 = CA PAM[{0}]: Unable to open connection to this resource  
 PAM-SPFD-0007 = CA PAM[{0}]: Lost access to remote storage. Connection closed.  
 PAM-SPFD-0008 = CA PAM[{0}]: Credentials for VNC SSO are invalid.  
 PAM-SPFD-0009 = CA PAM[{0}]: Fail to create session. Login session expired after {1} minute(s) of idle time.  
 PAM-SPFD-0010 = Invalid license.  
 PAM-SPFD-0011 = Current hosts ({0}) exceed licensed value ({1})  
 PAM-SPFD-0012 = CA PAM[{0}]: {1} connected to {2};{3}; Idle time out: {4};{5}  
 PAM-SPFD-0013 = CA PAM[{0}]: {1} initialized SSLVPN; {2}  
 PAM-SPFD-0014 = Failed to launch connection as the session recording can not be started.  
 PAM-SPFD-0015 = CA PAM[{0}]: Connection terminated; Duration: {1};{2}  
 PAM-SPFD-0016 = Failed to check certificate revocation status due to CRL expiration. Please update CRL.  
 PAM-SPFD-0017 = Preventing X-Forwarded-Host = {0}  
 PAM-SPFD-0018 = Preventing Cross Site Scripting Attempt  
 PAM-SPFD-0019 = FIPS module not included!  
 PAM-SPFD-0020 = FIPS module initialized!  
 PAM-SPFD-0021 = Session recording started for '{0}'. Triggered by CA Threat Analytics.  
 PAM-SPFD-0022 = Your session has been terminated. Contact your PAM Administrator.  
 PAM-SPFD-0023 = Applet Timed Out due to user inactivity  
 PAM-SPFD-0024 = Your connection to '{0}' {1} has been blocked by VMware NSX Security Policy.  
 PAM-SPFD-0025 = Error in prelogin call to '{0}' endpoint. Message: '{1}'  
 PAM-SPFD-0026 = Cannot set FIPS mode to {0}: {1}  
 PAM-SPFD-0027="CA PAM[{0}]: Starting processing of session recording;"  
 PAM-SPFD-0028="CA PAM[{0}]: Closing processing of session recording;"

## PAM-SRM: Session Recording Manager Messages

PAM-SRM-0000 = Graphical session recording: failed to access data base while writing file transfer event

PAM-SRM-0001 = Graphical session recording: Failed to access data base while writing Decryption key for hostId:{0} userID:{1}

PAM-SRM-0002 = Graphical session recording: failed to access data base while writing event with type {0} in recording file.

PAM-SRM-0003 = Graphical session recording: Failed to write general event in file : {0}

PAM-SRM-0004 = Graphical session recording: Failed to Complete recording for file : {0}

PAM-SRM-0005 = Graphical session recording: Failed to access database while writing file header for file : {0}

PAM-SRM-0006 = Graphical session recording: Failed to write file header for file : {0}BufferSize = {1}Bytes Written = {2}

PAM-SRM-0007 = Graphical session recording: Failed to write file header for file : {0}

PAM-SRM-0008 = Graphical session recording: Failed to update end time for file : {0}

PAM-SRM-0009 = Partially completed post-processing of session recording for {0}.

PAM-SRM-0010 = Completed post-processing of session recording for {0}.

PAM-SRM-0011 = An error occurred while post-processing of session recording: Can not process connect request. Probably security settings at remote server are too high. Deleting the file: {0}

PAM-SRM-0012 = An error occurred while post-processing of session recording: Recording file contains only file header packet. Possibly the remote server is powered off or security settings are too high. Deleting the file: {0}

PAM-SRM-0013 = An error occurred while post-processing of session recording: NLA login was canceled or invalid credentials were entered. Deleting the file: {0}

PAM-SRM-0014 = An error occurred while post-processing of session recording: Can't process TLS handshake. Deleting the file: {0}

PAM-SRM-0016 = Failed to synchronize NSX Securing Tags/Groups: wrong credentials

PAM-SRM-0017 = Failed to synchronize NSX Securing Tags/Groups: invalid NSX configuration

PAM-SRM-0018 = Failed to synchronize NSX Securing Tags/Groups: NSX manager response status code {0}

PAM-SRM-0019 = Failed to synchronize NSX Securing Tags/Groups: inner error

PAM-SRM-0020 = Failed to update ServiceManager of CA PAM Service: wrong credentials

PAM-SRM-0021 = Failed to update ServiceManager of CA PAM Service: invalid NSX configuration

PAM-SRM-0022 = Failed to update ServiceManager of CA PAM Service: NSX manager response status code {0}

PAM-SRM-0023 = Failed to update ServiceManager of CA PAM Service: inner error

PAM-SRM-0024 = Synchronization of security policies with VMware NSX completed successfully.

PAM-SRM-0025 = An error occurred while post-processing of session recording: Can't process TLS handshake. File: {0}

PAM-SRM-0026 = An error occurred while post-processing of session recording: {0} File: {1}

PAM-SRM-0027 = Failed to register CA PAM Service: wrong credentials

PAM-SRM-0028 = Failed to register CA PAM Service: invalid NSX configuration

PAM-SRM-0029 = Failed to register CA PAM Service: NSX manager response status code {0}

PAM-SRM-0030 = Failed to register CA PAM Service: inner error

PAM-SRM-0031 = Failed to unregister CA PAM Service: wrong credentials

PAM-SRM-0032 = Failed to unregister CA PAM Service: invalid NSX configuration

PAM-SRM-0033 = Failed to unregister CA PAM Service: NSX manager response status code {0}

PAM-SRM-0034 = Failed to unregister CA PAM Service: inner error

PAM-SRM-0035 = Failed to synchronize NSX security service: wrong credentials

PAM-SRM-0036 = Failed to synchronize NSX security service: invalid NSX configuration

PAM-SRM-0037 = Failed to synchronize NSX security service: NSX manager response status code {0}

PAM-SRM-0038 = Failed to synchronize NSX security service: inner error

PAM-SRM-0039 = Failed to add NSX firewall rule to unknown VM "{0}": wrong credentials

PAM-SRM-0040 = Failed to add NSX firewall rule to unknown VM "{0}": invalid NSX configuration

PAM-SRM-0041 = Failed to add NSX firewall rule to unknown VM "{0}": NSX manager response status code {1}

PAM-SRM-0042 = Failed to add NSX firewall rule to unknown VM "{0}": inner error

PAM-SRM-0043 = Failed to open access to {0}:{1} by adding NSX firewall rule: wrong credentials

PAM-SRM-0044 = Failed to open access to {0}:{1} by adding NSX firewall rule: invalid NSX configuration

PAM-SRM-0045 = Failed to open access to {0}:{1} by adding NSX firewall rule: NSX manager response status code {2}

PAM-SRM-0046 = Failed to open access to {0}:{1} by adding NSX firewall rule: inner error

PAM-SRM-0047 = Failed to remove NSX firewall rule: wrong credentials

PAM-SRM-0048 = Failed to remove NSX firewall rule: invalid NSX configuration

PAM-SRM-0049 = Failed to remove NSX firewall rule: NSX manager response status code {0}  
PAM-SRM-0050 = Failed to remove NSX firewall rule: inner error  
PAM-SRM-0051 = Starting post-processing of session recording {0}  
PAM-SRM-0052 = Failed post-processing of session recording {0}  
PAM-SRM-0053 = Session recording file {0} is inaccessible as primary network storage is down. Cannot start post-processing  
PAM-SRM-0054 = Session recording file {0} is inaccessible as failover network storage is down. Cannot start post-processing

## PAM-TELE: Telemetry Segment Messages

PAM-TELE-0001 = Unable to Save Telemetry Data. Proxy Server details provided for telemetry are invalid or it is not reachable.  
PAM-TELE-0002 = Unable to Submit Telemetry Data. There is an error connecting to the Telemetry server.  
PAM-TELE-0003 = Unable to Submit Telemetry Data. Proxy Server details provided for telemetry are invalid or it is not reachable.  
PAM-TELE-0004 = Telemetry details with PLA Agreement Enabled : {0}, Company Domain : {1}, Enterprise Site ID : {2}, Internal Identifier : {3}, Manual Feed : {4}, Proxy Enabled : {5} are saved.  
PAM-TELE-0005 = Identify call to Segment API is made with below details : {0}  
PAM-TELE-0006 = Track call to Segment API is made with below details : {0}  
PAM-TELE-0007 = This CA-PAM appliance is a member of a secondary site. Saving of Telemetry data is an admin function and must be performed from the primary site.

## PAM-UI: User Interface Messages

PAM-UI-0001 = Group Saved.  
PAM-UI-0003 = Group Deleted.  
PAM-UI-0004 = Context specific server error message. Module:ExampleFeature  
PAM-UI-0005 = Contact Saved.  
PAM-UI-0006 = Contact Deleted.  
PAM-UI-0007 = Context specific server error message. Module:ExampleFeature  
PAM-UI-0008 = Settings Saved.  
PAM-UI-0009 = Failed to load settings.  
PAM-UI-1001 = Item Saved.  
PAM-UI-1002 = Item Deleted.  
PAM-UI-1003 = Context specific server error message. Module:Common  
PAM-UI-1004 = User information has been updated  
PAM-UI-1005 = Authorization failed. User does not have permission for this action.  
PAM-UI-1006 = Search View deleted.  
PAM-UI-1007 = Error deleting search view.  
PAM-UI-1008 = Search View saved.  
PAM-UI-1009 = Communication failure.  
PAM-UI-1010 = Transaction aborted.  
  
PAM-UI-1100 = Request Group deleted.  
PAM-UI-1101 = Error deleting request group.  
PAM-UI-1102 = Request Group saved.  
PAM-UI-1103 = Script deleted.  
PAM-UI-1104 = Error deleting script.  
PAM-UI-1105 = Script saved.  
PAM-UI-1106 = Authorization Mapping deleted.  
PAM-UI-1107 = Error deleting authorization mapping.

PAM-UI-1108 = Authorization Mapping saved.  
PAM-UI-1110 = This client has not yet been authorized! Change the status to Active to authorize requests from this client.  
PAM-UI-1111 = Fingerprint update request was sent  
PAM-UI-1112 = Fingerprint update request failed  
PAM-UI-1113 = Change key update request was sent  
PAM-UI-1114 = Change key update request failed  
PAM-UI-1115 = All script hash update request was sent  
PAM-UI-1116 = All script hash update request failed  
PAM-UI-1117 = Script hash update request was sent  
PAM-UI-1118 = Script hash update request failed  
PAM-UI-1119 = Connection status check completed  
PAM-UI-1120 = Connection status check failed  
PAM-UI-1121 = Get log request was sent  
PAM-UI-1122 = Get log request failed  
PAM-UI-1200 = Error checking in password view  
PAM-UI-1201 = Password View checked in  
PAM-UI-1202 = Error getting access credentials  
PAM-UI-1203 = Error generating proxy account  
PAM-UI-1300 = AWS Connection Deleted.  
PAM-UI-1301 = AWS Connection Saved.  
PAM-UI-1302 = Context specific server error message. Module:Config  
PAM-UI-1303 = VMware vCenter Deleted.  
PAM-UI-1304 = VMware vCenter Saved.  
PAM-UI-1305 = Context specific server error message. Module:Config  
PAM-UI-1306 = RADIUS and TACACS+ Configuration Deleted.  
PAM-UI-1307 = RADIUS and TACACS+ Configuration Saved.  
PAM-UI-1308 = Context specific server error message. Module:Config  
PAM-UI-1309 = Splunk Configuration Deleted.  
PAM-UI-1310 = Splunk Configuration Saved.  
PAM-UI-1311 = Context specific server error message. Module:Config  
PAM-UI-1312 = LDAP Domain Deleted.  
PAM-UI-1313 = LDAP Domain Saved.  
PAM-UI-1314 = Context specific server error message. Module:Config  
PAM-UI-1315 = RSA Configuration File Deleted.  
PAM-UI-1316 = Context specific server error message. Module:Config  
PAM-UI-1317 = AWS API Proxy Auto-Activation Whitelist successfully updated.  
PAM-UI-1318 = Context specific server error message. Module:Config  
PAM-UI-1319 = NSX API Proxy Auto-Activation Whitelist successfully updated.  
PAM-UI-1320 = Context specific server error message. Module:Config  
PAM-UI-1321 = File deleted successfully. For this change to take effect, please restart Tomcat.  
PAM-UI-1322 = Context specific server error message. Module:Config  
PAM-UI-1323 = CA Threat Analytics configuration was successfully saved  
PAM-UI-1324 = CA Threat Analytic configuration was successfully cleared.  
PAM-UI-1325 = Successfully connected to CA Threat Analytic server  
PAM-UI-1326 = CASSO configuration was successfully saved. For this change to take effect, please restart Apache.  
PAM-UI-1327 = CA PAM Server Control configuration was successfully saved.  
PAM-UI-1328 = CA PAM Server Control configuration was successfully cleared.  
PAM-UI-1329 = Date/Time changed successfully.  
PAM-UI-1330 = Time Servers information updated successfully  
PAM-UI-1331 = NTP IFF key saved: {0} security policy {1}  
PAM-UI-1332 = Database file deleted successfully  
PAM-UI-1333 = Context specific server error message. Module:Config  
PAM-UI-1334 = CA PAM configuration restored successfully from file {0}. The CA PAM appliance is being rebooted.

PAM-UI-1335 = CA PAM database restored successfully from file {0}. The CA PAM appliance is being rebooted.

PAM-UI-1336 = Downloaded database file {0}

PAM-UI-1337 = Database dumped successfully; CA PAM configuration saved successfully

PAM-UI-1338 = The CA PAM database has been reset successfully. The CA PAM appliance is being rebooted.

PAM-UI-1339 = Database compacted. The CA PAM appliance is being rebooted.

PAM-UI-1340 = Database backup schedule saved successfully

PAM-UI-1341 = Database backup schedule deleted successfully

PAM-UI-1342 = {0} mount performed successfully

PAM-UI-1343 = {0} unmounting performed successfully

PAM-UI-1344 = Exception Rules Saved

PAM-UI-1345 = Set Time Successful

PAM-UI-1346 = Hardware Serial Saved

PAM-UI-1347 = License File Uploaded

PAM-UI-1348 = Successfully updated the monitoring configuration

PAM-UI-1349 = Monitor startup flag changed successfully

PAM-UI-1350 = Monitor started successfully

PAM-UI-1351 = Monitor stopped successfully

PAM-UI-1352 = The Automatic Log Purge Settings have been saved successfully.

PAM-UI-1353 = The External Log Settings have been saved successfully.

PAM-UI-1354 = Log file deleted successfully

PAM-UI-1355 = Context specific server error message. Module:Config

PAM-UI-1356 = Log records saved to file.

PAM-UI-1357 = Purged logs up till

PAM-UI-1358 = All logs have been purged

PAM-UI-1359 = Syslog configuration updated successfully

PAM-UI-1360 = Keystroke Logging configuration updated successfully

PAM-UI-1361 = {0} Mount settings saved successfully.

PAM-UI-1362 = Session Recording Preference saved successfully.

PAM-UI-1363 = Network settings updated successfully. Please reboot the appliance or click the Restart Networking button for the changes to take effect

PAM-UI-1364 = Network IPv4 Route Deleted

PAM-UI-1365 = Context specific server error message. Module:Config

PAM-UI-1366 = Network IPv6 Route Deleted

PAM-UI-1367 = Context specific server error message. Module:Config

PAM-UI-1368 = Network IPv4 Route Saved

PAM-UI-1369 = Network IPv6 Route Saved

PAM-UI-1370 = IP Address Deleted

PAM-UI-1371 = Context specific server error message. Module:Config

PAM-UI-1372 = IP Address Saved

PAM-UI-1373 = Certificate Revocation List deleted

PAM-UI-1374 = Error deleting Certificate Revocation List

PAM-UI-1375 = Session Recording Purge saved successfully.

PAM-UI-1376 = SNMP poll configuration saved successfully

PAM-UI-1377 = SNMP user saved successfully

PAM-UI-1378 = SNMP User Deleted

PAM-UI-1379 = Context specific server error message. Module:Config

PAM-UI-1380 = SNMP trap configuration saved successfully

PAM-UI-1381 = Management Console configuration was successfully saved.

PAM-UI-1382 = Management Console configuration was successfully cleared.

PAM-UI-1383 = Connected successfully to AWS.

PAM-UI-1384 = Connected successfully to vCenter.

PAM-UI-1385 = All the vCenter accounts provisioned are now Active.

PAM-UI-1386 = Updated config password



PAM-UI-1387 = Updated super user name  
PAM-UI-1388 = Network HSM Removed  
PAM-UI-1389 = Success initializing the internal LunaPCI-E device  
PAM-UI-1390 = Locale successfully saved. For this change to take effect, please restart the appliance.  
PAM-UI-1391 = Always Allow View Password on Secondary Site setting has been updated successfully  
PAM-UI-1392 = Refreshed Credential Manager Database Sync Status  
PAM-UI-1393 = Disabled because PAM is running in FIPS mode.  
PAM-UI-1394 = Cluster configuration was successfully reset  
PAM-UI-1395 = Cluster configuration reset failed  
PAM-UI-1396 = The AWS Refresh Interval has been saved.  
PAM-UI-1397 = The VMware Refresh Interval has been saved.  
PAM-UI-1398 = Success, you must reboot CA PAM for this change to take effect  
PAM-UI-1399 = Success updating the HSM password  
PAM-UI-1400 = Selected application must be of type LDAP, Active Directory, or Windows Proxy.  
PAM-UI-1401 = Success, updating the cryptography password.  
PAM-UI-1402 = FIPS Password Error  
PAM-UI-1403 = Cannot delete site: Cluster must have at least two members. Click RESET to delete the cluster.  
PAM-UI-1404 = Selected application must be of type RADIUS/TACACS+ Secret.  
PAM-UI-1405 = Please acknowledge the cluster warning message before powering off the appliance.  
PAM-UI-1406 = Please acknowledge the cluster warning message before rebooting the appliance.  
PAM-UI-1407 = Access settings saved  
PAM-UI-1408 = Success, CA PAM will now reboot for this change to take effect.  
PAM-UI-1409 = The IdP settings cannot be updated while the cluster is on  
PAM-UI-1410 = Sailpoint configuration settings have been saved  
PAM-UI-1411 = CA-PAM data has been exported to Sailpoint. See log for details  
PAM-UI-1412 = CA-PAM data has been imported from Sailpoint. See log for details  
PAM-UI-1413 = Sailpoint Integration tables have been installed.  
PAM-UI-1414 = KDC Server Configuration Deleted.  
PAM-UI-1415 = KDC Server Configuration Saved.  
PAM-UI-1416 = KDC failed  
PAM-UI-1417 = X Forwarded Host Check has been changed. This change requires an appliance restart to take effect.  
PAM-UI-1418 = The Azure Refresh Interval has been saved.  
PAM-UI-1419 = Azure Connection Deleted.  
PAM-UI-1420 = Azure Connection Saved.  
PAM-UI-1421 = Azure Connection Failed  
PAM-UI-1422 = Connected successfully to Azure.  
PAM-UI-1423 = No subscriptions available. Please make sure you have granted access to the PAM instance.  
PAM-UI-1424 = No resource groups available. Please make sure you have granted access to the PAM instance.  
PAM-UI-1425 = Azure MSI is not available! Please make sure Managed Service Identity has been enabled on the PAM instance in order to use Azure functionalities.  
PAM-UI-1426 = Azure MSI is not available! Please make sure Managed Service Identity has been enabled on the PAM instance in order to configure VIP properly  
PAM-UI-1427 = UI Logs Purged  
PAM-UI-1500 = Device Saved.  
PAM-UI-1501 = Device Deleted.  
PAM-UI-1502 = Context specific server error message. Module:Devices  
PAM-UI-1503 = Device Group Saved.  
PAM-UI-1504 = Device Group Deleted.  
PAM-UI-1505 = Context specific server error message. Module:Devices  
PAM-UI-1506 = Tag Saved.  
PAM-UI-1507 = Tag Deleted.  
PAM-UI-1508 = Context specific server error message. Module:Devices  
PAM-UI-1509 = Access Method Saved.

PAM-UI-1510 = Access Method Deleted.  
PAM-UI-1511 = Context specific server error message. Module:Devices  
PAM-UI-1512 = VMware devices refreshed  
PAM-UI-1513 = AWS devices refreshed  
PAM-UI-1514 = Device address is invalid  
PAM-UI-1801 = Error deleting policy.  
PAM-UI-1802 = Policy Saved.  
PAM-UI-1803 = Policy Deleted.  
PAM-UI-1804 = Error retrieving association information between user(group) and device(group).  
PAM-UI-1805 = Error deleting socket filter  
PAM-UI-1806 = Socket Filter Deleted.  
PAM-UI-1807 = Error deleting command filter  
PAM-UI-1808 = Policy Command Filter Deleted.  
PAM-UI-1809 = Command Filter Config Saved.  
PAM-UI-1810 = Socket Filter Config Saved.  
PAM-UI-1811 = Error deleting AWS policy.  
PAM-UI-1812 = AWS Policy Saved.  
PAM-UI-1813 = AWS Policy Deleted.  
PAM-UI-1814 = Policy Command Filter Saved.  
PAM-UI-1815 = Policy Socket Filter Saved.  
PAM-UI-1816 = Please assign the AWS policy to the Target Account {0}.  
PAM-UI-1901 = Error deleting Service.  
PAM-UI-1902 = Service Saved.  
PAM-UI-1903 = Service Deleted.  
PAM-UI-1904 = Error deleting Transparent Login Config.  
PAM-UI-1905 = Transparent Login Config Saved.  
PAM-UI-1906 = Transparent Login Config Deleted.  
PAM-UI-2001 = Discovered Device Updated.  
PAM-UI-2005 = Profile Job submitted  
PAM-UI-2006 = Profile Job failed:  
PAM-UI-2007 = Profile Job {0} Canceled.  
PAM-UI-2008 = Profile Job {0} Deleted.  
PAM-UI-2009 = Account Scan Profile Job Saved.  
PAM-UI-2010 = Account Scan Profile Job Deleted.  
PAM-UI-2011 = Context specific server error message. Module:Discovery  
PAM-UI-2012 = Account Profile Job submitted  
PAM-UI-2013 = Account Profile Job failed:  
PAM-UI-2014 = Manage Accounts failed:  
PAM-UI-2015 = Accounts were successfully managed.  
PAM-UI-2016 = Device Scan Profile Saved.  
PAM-UI-2018 = Device Scan Profile Deleted.  
PAM-UI-2019 = Context specific server error message. Module:Discovery  
PAM-UI-2020 = Context specific server error message. Module:Discovery  
PAM-UI-2021 = Update Accounts failed:  
PAM-UI-2022 = Accounts were successfully Updated.  
PAM-UI-2101 = Report Saved.  
PAM-UI-2102 = Report Deleted.  
PAM-UI-2103 = Context specific server error message. Module:Sessions  
PAM-UI-2200 = Alias deleted.  
PAM-UI-2201 = Error deleting alias.  
PAM-UI-2202 = Proxy deleted.  
PAM-UI-2203 = Error deleting proxy.  
PAM-UI-2204 = Proxy saved.

PAM-UI-2205 = Target Group deleted.  
PAM-UI-2207 = Target Group saved.  
PAM-UI-2209 = Error deleting target group.  
PAM-UI-2210 = Password Composition Policy deleted.  
PAM-UI-2211 = Error deleting password composition policy.  
PAM-UI-2212 = Password Composition Policy saved.  
PAM-UI-2213 = Could not read Request Server Global Settings.  
PAM-UI-2214 = Could not retrieve logs.  
PAM-UI-2215 = Fingerprint update request sent to proxy.  
PAM-UI-2216 = Key update request sent to proxy.  
PAM-UI-2217 = Request sent to get logs for request server. Please wait..  
PAM-UI-2218 = Could not read Fingerprint Settings.  
PAM-UI-2219 = SSH key pair policy deleted.  
PAM-UI-2220 = Error deleting SSH key pair policy.  
PAM-UI-2221 = SSH key pair policy saved.  
PAM-UI-2222 = Could not read SSH Key Pair Policy defaults.  
PAM-UI-2223 = Options OK. Sample SSH Key Pair Fingerprint:  
PAM-UI-2224 = Target Application saved.  
PAM-UI-2225 = Target Account saved  
PAM-UI-2226 = Target Account deleted  
PAM-UI-2227 = The Password View Request is approved.  
PAM-UI-2228 = Credential verification performed  
PAM-UI-2229 = Credential verification has failed  
PAM-UI-2230 = Unable to generate credential. No application is selected.  
PAM-UI-2231 = You have this account checked out.  
PAM-UI-2232 = Account has been checked in  
PAM-UI-2233 = Account check-in has failed  
PAM-UI-2234 = Service Host required  
PAM-UI-2235 = Service required  
PAM-UI-2236 = No services found.  
PAM-UI-2237 = {0} new services added of {1} discovered.  
PAM-UI-2238 = Task Host required  
PAM-UI-2239 = Task required  
PAM-UI-2240 = No task found.  
PAM-UI-2241 = {0} new tasks added of {1} discovered.  
PAM-UI-2242 = Service at line {0} requires a service host.  
PAM-UI-2243 = Service at line {0} requires a service name.  
PAM-UI-2244 = Task at line {0} requires a task host.  
PAM-UI-2245 = Task at line {0} requires a task name.  
PAM-UI-2246 = Required Remedy licensed files could not be found.  
PAM-UI-2247 = Updating passphrase will update the target account with newly generated key pair  
PAM-UI-2248 = No filters have been defined. Group must have at least one filter.  
PAM-UI-2301 = Could not read timezone regions.  
PAM-UI-2302 = Could not read user's current time.  
PAM-UI-2303 = Could not read server current time.  
PAM-UI-2304 = Could not read dashboard items.  
PAM-UI-2305 = Error deleting request server subnet.  
PAM-UI-2306 = Request Server Subnet Saved.  
PAM-UI-2307 = Request Server Subnet Deleted.  
PAM-UI-2308 = Request Server Settings Saved.  
PAM-UI-2309 = General Settings Saved.  
PAM-UI-2310 = Global Settings Saved  
PAM-UI-2311 = Email Settings Saved



PAM-UI-2316: SSH certificate policy deleted.  
PAM-UI-2317: Error deleting SSH certificate policy.  
PAM-UI-2318: SSH certificate policy saved.  
PAM-UI-2401 = Error deleting user.  
PAM-UI-2402 = User Saved.  
PAM-UI-2403 = User Deleted.  
PAM-UI-2404 = Error deleting group.  
PAM-UI-2405 = Group Saved.  
PAM-UI-2406 = Group Deleted.  
PAM-UI-2407 = Error deleting role.  
PAM-UI-2408 = Role Saved.  
PAM-UI-2409 = Role Deleted.  
PAM-UI-2410 = Error deleting CAC User.  
PAM-UI-2411 = Error approving CAC User.  
PAM-UI-2412 = CAC User Approved.  
PAM-UI-2413 = CAC User Deleted.  
PAM-UI-2414 = Error deleting Credential Manager role.  
PAM-UI-2415 = Credential Manager Role Saved.  
PAM-UI-2416 = Credential Manager Role Deleted.  
PAM-UI-2417 = Error deleting Credential Manager user group.  
PAM-UI-2418 = Credential Manager User Group Saved.  
PAM-UI-2419 = Credential Manager User Group Deleted.  
PAM-UI-2500 = Password view policy deleted.  
PAM-UI-2501 = Error deleting Password view policy.  
PAM-UI-2502 = Password view policy saved.  
PAM-UI-2503 = Required Remedy licensed files could not be found.  
PAM-UI-2504 = Reason Required For View must be selected when using Service Desk Integration.  
PAM-UI-2505 = Reason Required For Auto-Connect must be selected when using Service Desk Integration.  
PAM-UI-2506 = The Password View Requests have been deleted successfully.  
PAM-UI-2507 = Error deleting Password View Requests.  
PAM-UI-2508 = The Password View Requests have been approved.  
PAM-UI-2509 = Error approving Password View Requests.  
PAM-UI-2510 = The Password View Requests have been denied.  
PAM-UI-2511 = Error denying Password View Requests.  
PAM-UI-2600 = Scheduled Job deleted.  
PAM-UI-2601 = Error deleting Scheduled Job.  
PAM-UI-2602 = Scheduled Job saved.  
PAM-UI-2700 = Cluster information was saved.  
PAM-UI-2701 = Patch staging request was saved.  
PAM-UI-2702 = Patch information was saved.  
PAM-UI-2703 = Appliance information was deleted.  
PAM-UI-2704 = Appliance delete failed.  
PAM-UI-2705 = Cluster information was deleted.  
PAM-UI-2706 = Cluster update failed.  
PAM-UI-2707 = Cluster licenses were deleted.  
PAM-UI-2708 = Delete of cluster licenses failed.  
PAM-UI-2709 = Delete of patch information failed.  
PAM-UI-2710 = Patch information was deleted.  
PAM-UI-2711 = Patch staging recall request was saved.  
PAM-UI-2720 = The patch is already in the inventory: {0}  
PAM-UI-2721 = Bad SHA1 hash: {0}  
PAM-UI-2722 = Cannot decrypt patch file: {0}  
PAM-UI-2723 = Cannot read metadata file: {0}

PAM-UI-2724 = Missing metadata element: {0}  
PAM-UI-2725 = Cannot find patch metadata: {0}  
PAM-UI-2726 = Unknown archive file type: {0}  
PAM-UI-2727 = File upload succeeded: {0}  
PAM-UI-2728 = Could not extract files from uploaded ZIP: {0}  
PAM-UI-2729 = Patch file name does not match the package name: {0}

## PAM-UIL: UI Logging Messages

PAM-UIL-0001 = Could not obtain internal session ID. Task: {0}  
PAM-UIL-0002 = Purge task failed. Task: {0}  
PAM-UIL-0003 = Internal purge error. Task: {0}  
PAM-UIL-0004 = Failed to initialize purge task configuration. Task: {0}  
PAM-UIL-0005 = Task started: {0}  
PAM-UIL-0006 = Task completed: {0} Number of purged records: {1}

## PAM-UPD: Session Clean-up and Storage Status Messages

PAM-UPD-0001 = Closed expired session for user {0}.  
PAM-UPD-0002 = Terminating session for user {0}, as it is timed out!  
PAM-UPD-0003 = SAML session timed-out for user {0}.  
PAM-UPD-0004 = Session login timed-out for user {0}.  
PAM-UPD-0005 = There was a problem with the recording storage. This connection is not allowed in security-safe mode.  
PAM-UPD-0006 = This client has not responded to PAM messages. We have assumed the client has gone away, and the session is being reaped.  
PAM-UPD-0007 = There was a problem with PAM's connection to this client. There may be network issues, or the client may have gone away without properly logging out. This session will be cleaned up.  
PAM-UPD-0008 = There was a problem with PAM's connection to this client. There may be network issues, or the client may be not properly configured. Session data will be discarded.  
PAM-UPD-0009 = User {0} opened a Web Portal to {1} on {2}  
PAM-UPD-0010 = User {0} closed the Web Portal to {1} on {2}  
PAM-UPD-0012 = Your session has timed out.  
PAM-UPD-0013 = Primary network storage for session recording is up  
PAM-UPD-0014 = Primary network storage for session recording is down  
PAM-UPD-0015 = Failover network storage for session recording is up  
PAM-UPD-0016 = Failover network storage for session recording is down  
PAM-UPD-0017 = Network storage for database backup is up  
PAM-UPD-0018 = Network storage for database backup is down  
  
PAM-UPD-0019 = Network storage for database backup does not have enough free space!  
PAM-UPD-0020 = There was a problem with the recording storage. This connection is continued in operationally-safe mode.

## Credential Manager Client Return Codes

Credential Manager clients generate these return codes and the associated messages. These clients include A2A (application to application), Windows Proxy, Windows Remote, client integrations, and their associated components.

## **Message Headers**

- `error.validation.header` =Validation Error:
- `error.exception` =Exception occurred {0} in {1}
- `error.loadingEntity` =Unable to load entity of type {0} with id {1}
- `error.entityDoesNotExist` =The entity of type {0} with id {1} does not exist
- `error.entityNotCorrectType` =The retrieved entity of type {0} does not match the expected type of {1}

## **Error Codes and Associated Messages**

### ***General Messages***

- `error.code.0`=Success.
- `error.code.1`=Application error occurred.
- `error.code.2`=Failed to connect to database.
- `error.code.3`=Database version does not match application version.
- `error.code.4`=A database error occurred.
- `error.code.5`=Request failed. The Xsuite cluster is in stopped mode.
- `error.code.10`=Invalid user ID.
- `error.code.11`=Invalid password.
- `error.code.12`=Login failed.
- `error.code.13`=User ID/password combination does not exist.
- `error.code.14`=User session has not been authenticated. Please log in.
- `error.code.15`=Account suspended.
- `error.code.16`=Missing login digest values.
- `error.code.17`=Missing login digest.
- `error.code.18`=Cannot log in to secondary site.
- `error.code.19`=User is authenticated, but credential must be reset.
- `error.code.20`=User ID must have 3 to 16 characters.
- `error.code.21`=Password must have 6 to 16 characters.
- `error.code.22`=Authorization failed. User {0} does not have permission for this action.
- `error.code.23`=Password must contain at least one alpha character (a-z, A-Z).
- `error.code.24`=Password must contain at least one numeric character (0-9).
- `error.code.25`=Password must contain at least one special character (~!@#\$%^&\*()\_+~`~:~|~/?~.,).
- `error.code.26`=Authorization failed. User {0} does not have permission for this entity.
- `error.code.27`=Invalid password specified.
- `error.code.30`=Invalid license has been registered. Unable to complete request.
- `error.code.31`=License limit has been exceeded. Unable to complete request.
- `error.code.32`=Success. {Warning: Approaching license limit; you may need to upgrade your license.}
- `error.code.33`=Unlimited license error.
- `error.code.34`=Limited license error.
- `error.code.35`=Failed to register error. Error code already defined.
- `error.code.36`=Not authorized for updating the license. Permission required: `setSystemProperty`

### ***Client Error Messages***

- error.code.400=Success.
- error.code.401=Failed to authenticate with the Password Authority service.
- error.code.402=Unable to establish connection with client daemon.
- error.code.403=Not authorized (for client daemon).
- error.code.404=Unable to establish connection with Password Authority Server.
- error.code.405=No data found for specified target alias.
- error.code.406=An error occurred; if this problem persists then please ask your Administrator to investigate.
- error.code.407=Invalid parameters specified.
- error.code.408=Missing required parameter: {0}
- error.code.409=Unauthorized script name.
- error.code.410=Unauthorized execution path.
- error.code.411=Unauthorized execution user ID.
- error.code.412=Unauthorized request server.
- error.code.413=Error. Attempt to create a duplicate entry.
- error.code.414=Invalid target server specified.
- error.code.415=Invalid target application specified.
- error.code.416=Invalid account specified.
- error.code.417=Invalid request server specified.
- error.code.418=Invalid script specified.
- error.code.419=Invalid target alias specified.
- error.code.420=Invalid host name specified.
- error.code.421=Invalid IP address specified.
- error.code.422=Invalid port number specified. Unable to connect.
- error.code.423=Invalid execution path specified.
- error.code.424=Invalid script type specified.
- error.code.425=Invalid script name specified.
- error.code.426=Invalid execution user ID specified.
- error.code.427=Cannot update a new target alias.
- error.code.428=Maximum length of target alias exceeded.
- error.code.429=Application already exists for this server.
- error.code.430=No patch found.
- error.code.431=Patch found, but must be applied manually.
- error.code.432=Patch has already been processed.
- error.code.433=Privileged account cannot be used to create target alias.
- error.code.434=Invalid username.
- error.code.435=Invalid or no extension/application type specified.
- error.code.436=Security exception. Script integrity check failed.
- error.code.437=Security exception. Data tampering detected. Request denied.
- error.code.438=Unauthorized request server. Fingerprint has changed.
- error.code.439=Invalid XML definition.
- error.code.440=Password Authority Windows Proxy operation failed.
- error.code.441=Invalid file path specified.
- error.code.442=Unsupported command specified.
- error.code.446=Authorization mapping validation error. Invalid execution path specified for request script.
- error.code.447=Authorization mapping validation error. Invalid file path specified for request script.
- error.code.448=Authorization mapping validation error. Missing request script information.
- error.code.449=Authorization mapping validation error. Missing hash value for request script.
- error.code.450=Unsupported OS platform specified.
- ~~error.code.451=Command cannot be executed because the primary site is unavailable~~
- error.code.452=Primary site is unavailable. Any workflow tasks associated with the account's password view policy (dual authorization, change password, or checkin/checkout) have not been performed. <sup>2598</sup>
- error.code.460=Data source has not been initialized.
- error.code.461=Data source is not configured for clustering.
- error.code.462=Connection with client daemon timed out

**Native Call Application Error Messages**

- error.code.1400=Application JNI error - maximum length exceeded.
- error.code.1401=Application JNI error - null value.
- error.code.1500=Maximum retries exceeded.
- error.code.1501=No data found.
- error.code.1502=A problem occurred during archive. Not all records were archived. Please run the command again.

**Target Manager Error Messages**

- error.code.1600=Failed to synchronize password with target. If this problem persists then, please ask your Administrator to investigate.
- error.code.1601=Failed to verify password with target. If this problem persists then, please ask your Administrator to investigate.
- error.code.1602=Target server application is not responding!
- error.code.1603=Insufficient permission to change password on target application.
- error.code.1604=Authentication failed.
- error.code.1605=Database driver class not found.
- error.code.1606=Account is unsynchronized.
- error.code.1607=Target Manager cannot store credential
- error.code.1650=Unable to establish connection with target application!
- error.code.1651=Remote host closed connection during handshake. Possible invalid SSL certificate or port.
- error.code.1652=Invalid SSL Certificate.
- error.code.1660=Lock timeout, unable to process request.
- error.code.1661=Account update in progress, unable to process request.
- error.code.1662=The view password module did not respond.

**Role Error Messages**

- error.code.1700=Invalid role specified.
- error.code.1701=Role is read-only.
- error.code.1702=User status cannot be null.

**Update User Password Error Messages**

- error.code.1703=Invalid user password specified.
- error.code.1704=Invalid user authentication type.

**Client Error Messages**

- error.code.1800=Client is unable to process the request.
- error.code.1801=Unable to connect to client.
- error.code.1802=Client internal error processing request.
- error.code.1900=Invalid metric ID.

**Batch Sequence Error Messages**

- error.code.1910=Invalid parameters.
- error.code.1911=Invalid batch command.
- error.code.1912=Unable to commit transaction in database.
- error.code.1913=Unable to rollback transaction in database.
- error.code.1914=Unable to start a transaction in database.

- error.code.1920=Invalid start date
- error.code.1921=Invalid end date
- error.code.1922=Invalid result limit
- error.code.1930=Unable to upgrade database. Unsupported minimum release.
- error.code.1940=Another archive operation is in progress.
- error.code.1950=Invalid file name.
- error.code.1951=Invalid file path.
- error.code.1952=Invalid file permissions.
- error.code.1953=Invalid file size.
- error.code.1954=Invalid version when running in FIPS mode.

**Extension Manager: General Error Messages**

- error.code.2001=The password change process was not specified. The value assigned to the 'useOtherAccountToChangePassword' attribute must be 'true' or 'false'.
- error.code.2002=An invalid port number was specified.
- error.code.2003=An invalid Target Account ID was assigned to the 'otherAccount' attribute.
- error.code.2006=An invalid Target Account ID was assigned to the 'otherPrivilegedAccount' attribute.
- error.code.2007=The value assigned to the 'useOtherPrivilegedAccount' attribute must be 'true' or 'false'.

**Extension Manager: Oracle Error Messages**

- error.code.2011=Invalid database name.

**Extension Manager: UNIX Error Messages**

- error.code.2031=The specified other account has an incompatible protocol

**LDAP Error Messages**

- error.code.2041=No LDAP DN specified.

**Database Password Change Error Messages**

- error.code.2101=Invalid database username.
- error.code.2102=Invalid database password.
- error.code.2103=Invalid database host name.
- error.code.2104=Invalid database user type.
- error.code.2150=Failed to update database admin account.

**Enable Change-Password-On-View Error Messages**

- error.code.2201=Invalid interval parameter.

**Scheduling Error Messages**

- error.code.2301=Invalid schedule time.
- error.code.2302=This job will never run, the specified start date/time is in the past.
- error.code.2303=Failed to save job.
- error.code.2304=A Job already exists with this name.

**Constraint Error Messages**

- error.code.3000=Constraint manager parse error.
- error.code.3100=Invalid target server parameters.
- error.code.3200=Invalid target application parameters.
- error.code.3201=Cannot add a target application of a deprecated type.

### **Account Error Messages**

- error.code.3300=Invalid parameters.
- error.code.3301=Exceeded maximum length of access type parameter.
- error.code.3302=Account username may not contain whitespace characters.
- error.code.3303=Exceeded maximum length for username parameter.
- error.code.3304=Exceeded maximum length for password parameter.
- error.code.3305=The specified password view policy has "change password on view" enabled, but the account is unsynchronized.
- error.code.3306=The specified password view policy ID is invalid.
- error.code.3307=Duplicate compound servers are not allowed for compound account.
- error.code.3308=Circular reference. Account cannot refer to itself for "other account".
- error.code.3309=Target Server is not allowed to be added as compound server.
- error.code.3310=Compound account must be added as unsynchronized.
- error.code.3311=Servers are not specified for compound account.
- error.code.3312=Target server cannot be specified as a compound server.
- error.code.3313=Invalid target account ID.
- error.code.3314=User does not have `listOtherAccounts` permission.
- error.code.3315=The specified password view policy has "change password on SSO" enabled, but the account is unsynchronized.
- error.code.3316=Cannot use a password view policy with change on connection end with unsynchronized account.
- error.code.3317=Cannot use a password view policy with change on session end with unsynchronized account.
- error.code.3350=Password and confirm password do not match.
- error.code.3351=Account not specified.
- error.code.3360=Cannot update account password of unsynchronized account.

### **Target Alias Error Messages**

- error.code.3400=Invalid parameters.
- error.code.3401=Target alias name must consist only of characters [a-z A-Z 0-9 ~ \! @ \# \$ % ^ . \: \_ - + = \ / ].
- error.code.3500=Invalid request server parameters.
- error.code.3501=Request Server does not exist or has never connected to Password Authority Server.
- error.code.3502=Connection status checking is not supported on light clients.
- error.code.3503=Event polling is enabled or client port is invalid.
- error.code.3504=Invalid status code received from client ping.
- error.code.3505=Connection status checking is not supported on proxies.
- error.code.3506=Proxy cannot be deleted because it is in use.
- error.code.3507=Adding windows agent via CLI command is not supported in Xsuite.
- error.code.3508=Add request server failed.
- error.code.3600=Invalid script parameters.
- error.code.3700=Invalid script authorization parameters.
- error.code.3701=Invalid script authorization execution user maximum length exceeded.
- error.code.3702=Invalid script. It is on a different client than the one specified.
- error.code.3800=Invalid user parameters.

### **Role Error Messages**



- error.code.3900=Invalid parameters.
- error.code.3901=Exceeded maximum length of role name.
- error.code.3902=Role name must consist of characters [a-z, A-Z, 0-9].
- error.code.3903=Invalid role name.
- error.code.3904=Exceeded maximum length of role description.
- error.code.3905=Role description must consist of characters [a-z, A-Z, 0-9].
- error.code.3906=Invalid role ID.
- error.code.3907=Role is read-only.

**Group Error Messages**

- error.code.3950=Invalid parameters.
- error.code.3951=Exceeded maximum length of group name.
- error.code.3952=Group name must consist of characters [a-z, A-Z, 0-9].
- error.code.3953=Invalid group name.
- error.code.3954=Exceeded maximum length of group description.
- error.code.3955=Group description must consist of characters [a-z, A-Z, 0-9].
- error.code.3956=Invalid group ID specified.
- error.code.3957=Invalid permission specified.
- error.code.3958=Invalid object class ID.
- error.code.3959=Group is read-only.
- error.code.3960=Invalid group type.

**User Group Error Messages**

- error.code.3970=Invalid parameters.
- error.code.3971=Exceeded maximum length of user group name.
- error.code.3972=User group name must consist of characters [a-z, A-Z, 0-9].
- error.code.3973=Invalid user group name.
- error.code.3974=Exceeded maximum length of user group description.
- error.code.3975=User group description must consist of characters [a-z, A-Z, 0-9].
- error.code.3976=Invalid user group ID.
- error.code.3977=Invalid group IDs.
- error.code.3978=Invalid role ID.
- error.code.3979=User group is read-only.
- error.code.3980=Invalid read only.

**Report Error Messages**

- error.code.4000=Invalid parameters.

**System Property Error Messages**

- error.code.4100=Invalid property name specified.
- error.code.4101=Exceeded maximum length of property name.
- error.code.4102=Property name must consist of characters [a-z, A-Z, 0-9].
- error.code.4103=Invalid property value specified.

**E-mail Properties Validation Error Messages**



- error.code.4105=Invalid e-mail target account.
- error.code.4106=Invalid e-mail server host name.
- error.code.4107=Invalid e-mail server port.
- error.code.4108=Invalid e-mail address.
- error.code.4109=Invalid e-mail subject.
- error.code.4110=Invalid e-mail body.
- error.code.4111=Invalid e-mail subject for update.
- error.code.4112=Invalid e-mail body for update.
- error.code.4113=Target account not specified.
- error.code.4114=Requesting user not specified.
- error.code.4115=Password view policy not specified.
- error.code.4116=Password view request not specified.
- error.code.4117=Approver not specified.

### ***US 121 Messages***

- error.code.4118=Invalid e-mail subject for Password View.
- error.code.4119=Invalid e-mail body for Password View.

### ***US 120 Messages***

- error.code.4120=Invalid e-mail subject for Expired Password View Request.
- error.code.4121=Invalid e-mail body for Expired Password View Request.
- error.code.4122=Invalid e-mail subject for External Password Approvals.
- error.code.4123=Invalid e-mail body for External Password Approvals.

### ***US 91 Messages***

- error.code.4124=Invalid e-mail subject for Report Results.
- error.code.4125=Invalid e-mail body for Report Results.
- error.code.4126=Max User Group Limit cannot be more than 25.

### ***Initial Property Error Messages***

- error.code.4150=Invalid property name specified.

### ***Patch Error Messages***

- error.code.4200=Invalid patch ID.
- error.code.4201=Invalid request server ID.
- error.code.4202=Invalid patch detail ID.
- error.code.4203=Invalid activate all flag.
- error.code.4204=Patch already exists.
- error.code.4205=Patch deployment disabled.
- error.code.4206=Invalid Request Server connection status.
- error.code.4207=Release now only supported for request servers of version 4.5.2 and up.

### ***Password Policy Error Messages***

- error.code.4300=Invalid password policy ID.
- error.code.4301=Invalid password policy name.
- error.code.4302=Invalid password policy name.
- error.code.4303=Exceeded maximum length of password policy name.
- error.code.4304=Password policy name must consist of characters [a-z, A-Z, 0-9].
- error.code.4305=Exceeded maximum length of password policy description.
- error.code.4306=Password policy description must consist of characters [a-z, A-Z, 0-9].
- error.code.4307=Invalid password policy type, this is a required value.
- error.code.4308=Invalid password policy type value. Valid values [passwordPolicy].
- error.code.4309=Password policy special characters cannot contain XML characters (> < & ' ").
- error.code.4310=Password policy minimum length is too small.
- error.code.4311=Password policy maximum length is too small.
- error.code.4312=Minimum length must be less than the maximum length.
- error.code.4313=Policy validation error.
- error.code.4314=Password policy cannot be null.
- error.code.4315=Repeats cannot be allowed if duplicates are disallowed.
- error.code.4316=Select at least one character set in the 'Must Contain' category.
- error.code.4317=Select at least one character set in the 'First Must Contain' category.
- error.code.4318=First upper case character conflicts with no upper case characters anywhere.
- error.code.4319=First lower case character conflicts with no lower case characters anywhere.
- error.code.4320=First numeric character conflicts with no numeric characters anywhere.
- error.code.4321=First special character conflicts with no special characters anywhere.
- error.code.4322=Exclude characters, but none specified.
- error.code.4323=Include special characters, but none specified.
- error.code.4324=Include special first characters, but none specified.
- error.code.4325=Invalid special characters were specified anywhere in the password.
- error.code.4326=Invalid special characters were specified at the start of the password.
- error.code.4327=Excluded special characters were specified anywhere in the password.
- error.code.4328=Excluded special characters were specified at the start of the password.
- error.code.4329=Some first special characters are not allowed anywhere in the password.
- error.code.4330=No valid characters available. All have been excluded.
- error.code.4331=No valid first characters available. All have been excluded.
- error.code.4332=No valid first upper case characters available. All have been excluded.
- error.code.4333=No valid first lower case characters available. All have been excluded.
- error.code.4334=No valid first numeric characters available. All have been excluded.
- error.code.4335=No valid first special characters available. All have been excluded.
- error.code.4336=No valid upper case characters available. All have been excluded.
- error.code.4337=No valid lower case characters available. All have been excluded.
- error.code.4338=No valid numeric characters available. All have been excluded.
- error.code.4339=No valid special characters available. All have been excluded.
- error.code.4340=Password prefix contains excluded first character.
- error.code.4341=Password prefix contains excluded characters.
- error.code.4342=Password prefix cannot contain duplicate characters.
- error.code.4343=Password prefix cannot contain repeating adjacent characters.
- error.code.4344=Invalid policy type.
- error.code.4345=Unrecognized policy type.
- error.code.4346=Must specify a Policy ID or Name but not both.
- error.code.4347=No policies were deleted.
- error.code.4348=No policies were found
- error.code.4350=Specified password does not conform to the set password policy.
- error.code.4351=Password policy could not be found for parent application.
- error.code.4352=Failed to generate a password for the specified policy!
- error.code.4353=Password does not meet the minimum length requirement.
- error.code.4354=Password exceeds the maximum allowed length.

- error.code.4500=Authentication module configuration error.
- error.code.4501=Authentication module not found.
- error.code.4502=Authentication XML invalid.

- error.code.4600=Password view policy name is invalid.
- error.code.4601=Password view policy name is too long.
- error.code.4602=Password view policy name contains invalid characters.
- error.code.4603=Password view policy description is too long.
- error.code.4604=Password view policy description contains invalid characters.
- error.code.4605=Invalid value for change password on view was specified. Valid values are "true" or "false".
- error.code.4606=Invalid value for change password interval was specified. Numeric value between 1 and 525600 must be specified.
- error.code.4607=Invalid value for checkout / checkin required was specified. Valid values are "true" or "false".
- error.code.4608=Invalid value for checkout / checkin interval was specified. Numeric value between 1 and 525600 must be specified.
- error.code.4609=Invalid value for dual authorization required was specified. Valid values are "true" or "false".
- error.code.4610=Invalid value for dual authorization interval was specified. Numeric value between 1 and 525600 must be specified.
- error.code.4611=Invalid PasswordViewPolicy.ID was specified.
- error.code.4612=Approvers must be specified if dual authorization is enabled in the policy.
- error.code.4613=Invalid list of approvers was specified.
- error.code.4614=Password view policy is read-only.
- error.code.4615=The specified password view policy name is already in use.
- error.code.4616=Password view policy approvers are not able to access the target account(s) that use this policy.
- error.code.4617=One or more of the approvers in this policy are unable to update password view requests.
- error.code.4618=This account is checked out by another user.
- error.code.4619=This account is checked out and cannot be updated.
- error.code.4620=This account is checked out by a different user.
- error.code.4621=You have this account checked out.
- error.code.4622=The specified password view request does not exist.
- error.code.4623=The password request dates specified are invalid.
- error.code.4624=You have a pending request to view this account password that has not been approved yet.
- error.code.4625=This account has dual authorization enabled. A request for authorization to view the password has been e-mailed to the approvers of this account on your behalf.
- error.code.4626=Password view policy is in use and cannot be deleted.
- error.code.4627=Your account password request has been approved, but you are outside the approval period.
- error.code.4628=Password view policy has "change password on view" enabled, but the account is unsynchronized. Password will not be changed.
- error.code.4629=The specified status is invalid. Allowed values for Dual Authorization are approved(1), denied(2), pending(3), expiredapproved (6), or expiredpending (8). For Check-out/ Check-in the values are checkout (4), checkedin (5).
- error.code.4630=Invalid value for authentication required was specified. Valid values are "true" or "false".
- error.code.4631=The above error occurred updating the account password, but the account has still been checked in.
- error.code.4632=Cannot check out synchronized accounts that are unverified.
- error.code.4633=Users must be specified if Email notification is enabled in the policy.
- error.code.4634=Invalid value for email notification required was specified. Valid values are "true" or "false".
- error.code.4635=Email notification failed to some of the Users.
- error.code.4636=Checkin/checkout interval should be less than or equal to Dual authorization interval.
- error.code.4637=Start and/or end date is outside the maximum allowable request period.Requests cannot be made more than {0} days in the future.
- error.code.4638=Max duration is {0} minutes.
- error.code.4639=Invalid Enable One Click Approval Value.
- error.code.4640=The default password view request interval must be equal or less than the maximum password view request interval
- error.code.4641=Missing start date parameter.
- error.code.4642=Missing end date parameter.
- error.code.4643=Start date must not be in the past by up to 10 minutes.
- error.code.4644=End date must not be in the past.
- error.code.4645=Start date must be before end date.

- error.code.4690=Password request is only approved for View (not Auto-Connect).
- error.code.4691=Password request is only approved for Auto-Connect (not View).
- error.code.4692=Password request is only approved for different Auto-Connect type.
- error.code.4693=Invalid value for "Reason Required For View" was specified. Valid values are "true" or "false".
- error.code.4694=Invalid value for "Reason Required For Auto-Connect" was specified. Valid values are "true" or "false".
- error.code.4695=Invalid Service Desk Type specified.
- error.code.4696=Reason Required For View and Reason Required For Auto-Connect are required when Service Desk integration is specified.
- error.code.4698=Password view policy has "Change Password on Auto-Connect" enabled, but the account is unsynchronized. Password will not be changed.
- error.code.4699=Invalid value for allow "Change Password on Auto-Connect" was specified. Valid values are "true" or "false".
- error.code.4700=Crypto Application error.
- error.code.4701=Failed to find crypto provider class.
- error.code.4702=Failed to instantiate crypto provider class.
- error.code.4703=Failed to retrieve server encryption key.
- error.code.4704=Failed to set server encryption key.
- error.code.4705=Failed to generate a server key.
- error.code.4706=Failed to decrypt ciphertext.
- error.code.4707=Failed to encrypt cleartext.
- error.code.4708=Failed to retrieve current server key.
- error.code.4709=Application error - Object does not contain `cspm_serverkey` attribute.
- error.code.4710=Need to decrypt prior to encrypting.
- error.code.4711=Key change in progress
- error.code.4712=Invalid key
- error.code.4800=Invalid interval for change password.
- error.code.4801=Invalid List Page Size.
- error.code.4850=Auto-Connect validation unknown error.
- error.code.4851=Auto-Connect validation permission error.
- error.code.4852=Auto-Connect validation rollback error.
- error.code.4853=Auto-Connect invocation unknown error.
- error.code.4854=Auto-Connect invocation permission error.
- error.code.4855=Auto-Connect invocation rollback error.
- error.code.4856=Auto-Connect denied by target connector.
- error.code.4857=Auto-Connect user does not match target account.
- error.code.4858=Auto-Connect parameter is missing.
- error.code.4859=Auto-Connect parameter is not editable.
- error.code.4860=Auto-Connect port range is 1-65535.
- error.code.4861=Auto-Connect denied by target application.
- error.code.4862=Auto-Connect SSO type unknown for target application.

- error.code.4900=Must specify site name, site type and host name.
- error.code.4901=Must specify one of site name, site type, or host name.
- error.code.4902=Only one primary site can be provisioned in the system.
- error.code.4903=A site with the specified name already exists.
- error.code.4904=The specified site is not in the database.
- error.code.4905=The site ID to delete was not specified.
- error.code.4906=The specified site type is invalid.
- error.code.4907=The site ID to update was not specified.
- error.code.4908=Only this site can be set as the primary site.
- error.code.4909=Failed to retrieve local site information.
- error.code.4910=Failed to retrieve local site name.
- error.code.4911=Cannot provision a secondary site until the primary site has been provisioned.
- error.code.4912=Primary site cannot be deleted while secondary sites exist.
- error.code.4913=No changes to the primary site may be performed.
- error.code.4950=An error occurred during replication; please ask your Administrator to investigate.
- error.code.4951=Secondary site out of sync with primary. Secondary site has higher replication record than primary.
- error.code.4952=Secondary site does not have minimum replication record.
- error.code.4953=Primary site error while processing secondary site request (serialization).
- error.code.4954=Primary site error while processing secondary site request (I/O).
- error.code.4955=Primary site error while processing secondary site request (class not found).
- error.code.4956=Primary site error while processing secondary site request (execute command request).
- error.code.4957=Primary site error while processing secondary site request (proxy command requests).
- error.code.4960=Host name checking has not been disabled.
- error.code.4965=The Row Limit provided is invalid.
- error.code.4970= Password View Request Delete Interval Days is invalid.
- error.code.4980=The client is offline.
- error.code.4981=Unable to confirm whether or not the client is online.
- error.code.4982=The client is online.
- error.code.4984=Invalid current password specified.
- error.code.4985=The password confirm field doesn't match the new password.
- error.code.4986=The new password is the same as current password.
- error.code.4997=Invalid URL characters
- error.code.4998=URL maximum length exceeded
- error.code.4999=Cannot invoke command from remote host: {s}

**Error Code Messages Common to Multiple Target Connectors and Authenticators**

- error.code.5000=Account is disabled
- error.code.5001=Account is locked
- error.code.5002=Account's password is expired on target
- error.code.5003=Account is expired
- error.code.5004=Must reset the password
- error.code.5005=Account not found
- error.code.5006=Not permitted to logon from workstation

- error.code.5050=Internal target connector error.
- error.code.5051=Change process not specified.
- error.code.5052=No agent specified.
- error.code.5053=Invalid domain specified.
- error.code.5054=Failed to connect to agent.
- error.code.5055=The computer name is invalid.
- error.code.5056=The operation is allowed only on the primary domain controller of the domain.
- error.code.5057=The user name could not be found.
- error.code.5058=Password error. (The password could be too short, be too long, be too recent in its change history, not have enough unique characters, or not meet another password policy requirement.).
- error.code.5059=Validation failed. The password is invalid.
- error.code.5060=Could not find the domain controller for the domain.
- error.code.5061=Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirement of the domain.
- error.code.5062=Logon failure: unknown user name or bad password.
- error.code.5063=Configuration information could not be read from the domain controller, either because the machine is unavailable, or access has been denied.
- error.code.5064=The specified network account name or password is not correct.
- error.code.5064=The specified network account name or password is not correct.
- error.code.5065=The CSPM Windows Agent is not active.
- error.code.5066=The CSPM Windows Agent is not responding.
- error.code.5067=Failed to update the services.
- error.code.5068=Agent reports invalid operation.
- error.code.5069=Agent has never registered.
- error.code.5070=The specified service does not exist as an installed service.
- error.code.5071=Agent error - Invalid handle.
- error.code.5072=Agent error - The specified database does not exist.
- error.code.5073=Agent error - The data area passed to a system call is too small.
- error.code.5074=The RPC server is unavailable.
- error.code.5075=Password verification failed. Failed to connect to user account.
- error.code.5076=Password verification failed. Failed to set security.
- error.code.5077=No such login session.
- error.code.5078=Bad net path.
- error.code.5079=Service rollback failed.
- error.code.5080=Service rollback successful.
- error.code.5081=Host name and service name must have 1 to 100 characters and must not contain special characters.
- error.code.5082=Force password change attribute is incorrect.
- error.code.5083=Administrator account not specified.



- error.code.5100=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.5101=Failed to load the default or revised update script file.
- error.code.5102=Failed to load the default or revised verify script file.
- error.code.5103=Failed to update the account credentials. Review the log file for further information or else contact your Administrator.
- error.code.5104=Failed to verify the account credentials. Review the log file for further information or else contact your Administrator.
- error.code.5105=Cannot use another account's credentials to verify this account's credentials; the operation is not supported.
- error.code.5106=Failed to enter into privileged EXEC mode. Review the log file for further information or else contact your Administrator.
- error.code.5107=Failed to commit running configuration; the password has changed in running configuration only. Review the log file for further information or else contact your Administrator.
- error.code.5108=Failed to restore running configuration from start up configuration. Review the log file for further information or else contact your Administrator.
- error.code.5110=The private key is missing from the request.
- error.code.5111=An invalid private key was specified.
- error.code.5112=The public key is missing from the request.
- error.code.5113=An invalid public key was specified.
- error.code.5120=An invalid Cisco variant was specified.
- error.code.5121=Must specify a host key.
- error.code.5122=An invalid SSH port number was specified; the value must be in the range 0.65535.
- error.code.5123=The value assigned to the 'sshUseDefaultKeyExchangeAlgorithms ' attribute must be 'true' or 'false'.
- error.code.5124=Must NOT specify list of key exchange algorithms because default algorithms will be used instead.
- error.code.5125=The value assigned to the 'sshUseDefaultCompressionAlgorithms ' attribute must be 'true' or 'false'.
- error.code.5126=Must NOT specify list of compression algorithms because default algorithms will be used instead.
- error.code.5127=The value assigned to the 'sshUseDefaultServerHostKeyAlgorithms ' attribute must be 'true' or 'false'.
- error.code.5128=Must NOT specify list of server host key algorithms because default algorithms will be used instead.
- error.code.5129=An invalid Telnet port number was specified; the value must be in the range 0.65535.
- error.code.5130=An invalid SSH communication timeout was specified; the value must be in the range 1000.99999.
- error.code.5132=An invalid script processor read timeout was specified; the value must be in the range 1000.59999.
- error.code.5133=The value assigned to the 'sshStrictHostKeyCheckingEnabled ' attribute must be 'true' or 'false'.
- error.code.5135=The value assigned to the 'useUpdateScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.
- error.code.5136=The value assigned to the 'useVerifyScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.
- error.code.5137=The value assigned to the 'sshUseDefaultCiphers ' attribute must be 'true' or 'false'.
- error.code.5138=Must NOT specify list of ciphers because default ciphers will be used instead.
- error.code.5139=An invalid Telnet communication timeout was specified; the value must be in the range 1000.99999.
- error.code.5140=The value assigned to the 'sshUseDefaultHashes ' attribute must be 'true' or 'false'.
- error.code.5141=Must NOT specify list of hashes because default ciphers will be used instead.
- error.code.5170=An invalid protocol was specified.
- error.code.5171=Must specify a protocol.
- error.code.5172=Must specify a password type.
- error.code.5173=The value assigned to the 'pwType ' attribute must be 'user' or 'privileged'.
- error.code.5174=Must specify whether or not to change the AUX password.
- error.code.5175=The value assigned to the 'changeAuxLoginPassword ' must be 'true' or 'false'.
- error.code.5176=Must specify whether or not the change the Console password.
- error.code.5177=The value assigned to the 'changeConsoleLoginPassword ' must be 'true' or 'false'.
- error.code.5178=Must specify whether or not to change the VTY password.



- error.code.5200=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.5240=Change process not specified.
- error.code.5241=Must specify an 'other account'.
- error.code.5242=Must specify whether the account will be verified through another account.
- error.code.5243=The value assigned to the 'verifyThroughOtherAccount ' attribute must be 'true' or 'false'.
- error.code.5250=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.5251=An invalid LDAP connect timeout was specified; the value must be in the range 1000.99999.
- error.code.5252=An invalid LDAP read timeout was specified; the value must be in the range 1000.99999.
- error.code.5253=Must specify a protocol.
- error.code.5254=An invalid protocol was specified.
- error.code.5255=An invalid port number was specified; the value must be in the range 0.65535.
- error.code.5256=You must specify an SSL certificate.
- error.code.5301=An invalid port number was specified; the value must be in the range 0.65535.
- error.code.5302=Schema not specified.
- error.code.5303=Change process not specified.
- error.code.5304=Incorrect value specified for `racService` attribute. Valid values are true or false.
- error.code.5305=Incorrect value specified for `sysdbaAccount` attribute. Valid values are true or false.
- error.code.5306=Incorrect value specified for `replaceSyntax` attribute. Valid values are true or false.
- error.code.5307=Invalid value for SSL Enabled.
- error.code.5308=Invalid Crystal Reports database list specified.
- error.code.5310=Failed to synchronize/verify account. See logs for details.
- error.code.5311=Account locked.
- error.code.5312=Failed to connect to host.
- error.code.5313=Invalid schema/SID specified.
- error.code.5314=Failed to synchronize/verify account. Login failed.
- error.code.5315=Failed to synchronize Crystal Reports credentials. See logs for details.
- error.code.5500=Invalid port number.
- error.code.5501=Change process not specified.
- error.code.5502=Invalid value for SSL Enabled.
- error.code.5510=Failed to synchronize/verify account. See logs for details.
- error.code.5511=Failed to connect to database. Connection refused.
- error.code.5512=Failed to connect to database. Unknown host.
- error.code.5513=Communication failure. The target server must be SQL Server 2000 or later.
- error.code.5514=Invalid character in password. Single quotation mark (') is not a valid password character.
- error.code.5515=Failed to connect to database. Login failed.
- error.code.5500=Invalid port number.
- error.code.5501=Change process not specified.
- error.code.5504=Invalid Crystal Reports Server host name specified.
- error.code.5505=Invalid Crystal Reports Server port specified.
- error.code.5506=Invalid Crystal Reports Server application name specified.
- error.code.5507=Invalid Crystal Reports Server account name specified.
- error.code.5508=Invalid Crystal Reports database list specified.

- error.code.5510=Failed to synchronize/verify account. See logs for details.
- error.code.5511=Failed to connect to database. Connection refused.
- error.code.5512=Failed to connect to database. Unknown host.
- error.code.5513=Communication failure. The target server must be SQL Server 2000 or later.
- error.code.5514=Invalid character in password. Single quotation mark (') is not a valid password character.
- error.code.5515=Failed to synchronize Crystal Reports credentials. See logs for details.
- error.code.5550=Domain name must be specified.
- error.code.5551=Cannot retrieve Distinguished Name (DN).
- error.code.5552=Distinguished Name (DN) must be specified.
- error.code.5553=Cannot retrieve list of DNS servers.
- error.code.5554=Could not find any host name.
- error.code.5555=Cannot connect to a domain controller on specified domain.
- error.code.5556=Value for 'getDNS ' attribute must be specified.
- error.code.5557=Unknown option specified for protocol.
- error.code.5558=SSL certificate must be specified.
- error.code.5559=Value for 'useDN ' attribute must be specified.
- error.code.5560=Invalid value for 'appendDC ' attribute.
- error.code.5330=Change process not specified.
- error.code.5331=An 'other account' must be specified.
- error.code.5340=Unable to verify the password due to an error.
- error.code.5341=Unable to verify the password because the account is locked.
- error.code.5342=Unable to verify the password; failed to connect to the target server.
- error.code.5343=Verification failed because the password was not accepted.
- error.code.5344=Unable to update the password due to an error.
- error.code.5401=Invalid port specified.
- error.code.5402=Change process not specified.
- error.code.5403=Invalid value for SSL Enabled.
- error.code.5410=Failed to synchronize/verify account. See logs for details.
- error.code.5411=Failed to connect to database.
- error.code.5412=Failed to synchronize/verify account. Login failed.
- error.code.5450=Failed to synchronize/verify account. See logs for details.
- error.code.5451=Failed to connect to host.
- error.code.5601=Invalid port specified in target application for update script.
- error.code.5602=Invalid login account specified in target application.
- error.code.5603=Expect script for updating not specified in target application.
- error.code.5604=Invalid timeout value specified for update script in target application.
- error.code.5605=Invalid port specified in target application for verify script.
- error.code.5606=Expect script for verification not specified in target application.
- error.code.5607=Invalid timeout value specified for verify script in target application.
- error.code.5610=Failed to connect to host.
- error.code.5611=Failed to synchronize.
- error.code.5612=Unexpected error.

- error.code.5650=Invalid port specified.
- error.code.5651=Database name not specified.
- error.code.5652=Change process not specified.
- error.code.5670=Failed to synchronize/verify account. See logs for details.
- error.code.5671=Failed to connect to host.
- error.code.5672=Failed to synchronize/verify account. Login failed.
- error.code.5750=Domain name must be specified.
- error.code.5751=Distinguished Name (DN) must be specified.
- error.code.5753=Cannot connect to a domain controller on the specified domain.
- error.code.5754=Certificate cannot be retrieved from the domain controller.
- error.code.5755=Error storing certificate in certificate store.
- error.code.5756=Proxy host name is invalid:.
- error.code.5757=Error updating service credentials. See log for more information.
- error.code.5758=Services could not be restarted.
- error.code.5759=Error updating password in Active Directory. Service credentials for this account (if any) were not updated.
- error.code.5760=Error verifying services.
- error.code.5761=Cannot retrieve DNS host name(s).
- error.code.5762=Unknown option specified for "useDNS " attribute.
- error.code.5763=DNS server name not specified.
- error.code.5764=Distinguished Name (DN) must be specified.
- error.code.5765=Failed to update the services.
- error.code.5766=Invalid boolean value for Disable Auto-Connect Target Account.
- error.code.5767=Domain controller's root distinguished name could not be found.
- error.code.5768=One or more groups could not be found on domain controller.
- error.code.5769=An error occurred when discovering accounts on the domain controller.
- error.code.5770=Group names not specified.
- error.code.5771=Login account not specified.
- error.code.5772=Error updating task credentials. See log for more information.
- error.code.5773=An invalid LDAP connect timeout was specified; the value must be in the range 1000.99999.
- error.code.5774=An invalid LDAP read timeout was specified; the value must be in the range 1000.99999.

**Error Code Messages for Remedy Target Manager Connector (5800 through 5819)**

- error.code.5800=Change process not specified.
- error.code.5801=Change process not specified.
- error.code.5802=Internal target connector error.
- error.code.5803=Failed to synchronize password with target.
- error.code.5804=Failed to verify password with target.
- error.code.5805=Remedy server specified in the target application could not be found.
- error.code.5806=A port must be specified.
- error.code.5807=A BMCRemedyClientURL must be specified.
- error.code.5808=Required Remedy licensed files could not be found.
- error.code.5809=Could not log into Remedy server.

- error.code.5820=Failed to verify account in CSPM.
- error.code.5821=Failed to update account in CSPM.
- error.code.5822=Account password does not adhere to password policy.
- error.code.5823=User not found.
- error.code.5824=User uses external authentication. Password can not be updated.
- error.code.5825=Failed to connect to CSPM Server.
- error.code.5850=System Number not specified.
- error.code.5851=Invalid numeric value for System Number.
- error.code.5852=Client not specified.
- error.code.5853=Invalid numeric value for Client.
- error.code.5854=Additional Parameters must be a list of name=value pairs separated by semicolon.
- error.code.5860=Internal target connector error.
- error.code.5861=Failed to synchronize password with target.
- error.code.5862=Failed to verify password with target.
- error.code.5863=Failed to load native library.
- error.code.5864=Failed to connect to target system. Communication error.
- error.code.5865=BAPI User Change Function not found.
- error.code.5866=BAPI User Change Password Function not found.
- error.code.5867=Login Failure. See logs for details.
- error.code.5900=Telnet host name not specified.
- error.code.5901=Invalid port.
- error.code.5902=Invalid login account specified in target application.
- error.code.5903=Java not specified.
- error.code.5910=Failed to connect to host.
- error.code.5911=Failed to synchronize.
- error.code.5912=Unexpected error.
- error.code.5913=Script evaluation error. See logs for details.
- error.code.5950=Invalid port number.
- error.code.5951=Change process not specified.
- error.code.5954=Invalid Crystal Reports Server host name specified.
- error.code.5955=Invalid Crystal Reports Server port specified.
- error.code.5956=Invalid Crystal Reports Server application name specified.
- error.code.5957=Invalid Crystal Reports Server account name specified.
- error.code.5958=Invalid Crystal Reports database list specified.
- error.code.5959=Invalid database port specified.
- error.code.5960=Invalid database specified.
- error.code.5961=Invalid port specified.
- error.code.5962=Invalid value for 'isRootAccount '.
- error.code.5963=An invalid SSH communication timeout was specified; the value must be in the range 1000.99999.
- error.code.5964=An invalid script processor read timeout was specified; the value must be in the range 1000.59999.
- error.code.5965=The value assigned to the 'sshStrictHostKeyCheckingEnabled ' attribute must be 'true' or 'false'.
- error.code.5966=An invalid UID/GID number was specified; the value must be in the range 0.65535.

- error.code.5973=Failed to synchronize Crystal Reports credentials. See logs for details.
- error.code.5976=Must specify whether the account will be verified through another account.
- error.code.5977=The value assigned to the 'verifyThroughOtherAccount ' attribute must be 'true' or 'false'.
- error.code.5979=The value assigned to the 'useUpdateScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.
- error.code.5982=The value assigned to the 'useVerifyScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.
- error.code.5984=Must specify an 'other account'.
- error.code.5986=Must specify a protocol.
- error.code.5987=The value assigned to the 'sshUseDefaultCiphers ' attribute must be 'true' or 'false'.
- error.code.5988=Must NOT specify list of ciphers because default ciphers will be used instead.
- error.code.5989=The value assigned to the 'enableChannelDebugging ' attribute must be 'true' or 'false'.
- error.code.5990=An invalid Telnet communication timeout was specified; the value must be in the range 1000.99999.
- error.code.5995=Failed to update the account credentials. Review the log file for further information or else contact your Administrator.
- error.code.5996=Failed to verify the account credentials. Review the log file for further information or else contact your Administrator.
- error.code.5997=The value assigned to the 'sshUseDefaultHashes ' attribute must be 'true' or 'false'.
- error.code.5998=Must NOT specify list of hashes because default ciphers will be used instead.
- error.code.6000=Invalid port specified.
- error.code.6001=Change process not specified.
- error.code.6002=Database name not specified.
- error.code.6003=Invalid host\_name qualifier.
- error.code.6004=Max length exceeded for field sampleProperty .
- error.code.6005=Field useOtherAccount is mandatory.
- error.code.6006=SampleProperty is mandatory.
- error.code.6007=Max length exceeded for field sampleProperty .
- error.code.6008=Custom error message.
- error.code.6010=Failed to synchronize/verify account. See logs for details.
- error.code.6011=Account locked.
- error.code.6012=Failed to connect to host.
- error.code.6013=Failed to synchronize/verify account. Login failed.
- error.code.6014=Failed to update account. Access violation for account. Check target server or host\_name qualifier.

- error.code.6101=A Credential Type must be specified.
- error.code.6102=An unrecognized Credential Type was specified.
- error.code.6103=A Secret Access Key is required.
- error.code.6104=The Access Key ID must be composed with upper case letters, digits and must be 20 characters in length.
- error.code.6105=The Secret Access Key must be composed with alphanumeric, "+", "/" characters and must be 40 characters in length.
- error.code.6106=The uploaded EC2 Private Key file does not contain a PEM-formatted certificate.
- error.code.6107=An Access Key ID is required.
- error.code.6108=An X.509 certificate file name is required.
- error.code.6109=The X.509 certificate file name must match the pattern "pk-[A-Z0-9]{32}.pem". Example: "pk-4QUDAEWQENET2S22ABOOJ4BMUN6AUZY5.pem".
- error.code.6110=A PEM-formatted certificate file containing the EC2 Private Key must be uploaded.
- error.code.6111=An EC2 Instance User Name is required.
- error.code.6113=The IAM User Name is formatted incorrectly.
- error.code.6114=A Key Pair Name may be specified only when the Credential Type is EC2 Private Key.
- error.code.6115=A Key Pair Name is required.
- error.code.6116=The EC2 Instance User Name is formatted incorrectly or it contains the disallowed "@" character.
- error.code.6117=The Key Pair Name may not contain the "@" character.
- error.code.6118=An User Friendly Account Name is required.
- error.code.6119=Duplicated User Friendly Account Name.
- error.code.6120=Maximum length of AWS access role name exceeded.
- error.code.6121=AWS access role name only allows alphanumeric and '+=, @-' characters.
- error.code.6122=The AWS Cloud Type must be specified.
- error.code.6123=The maximum length of AWS Cloud Type exceeded.
- error.code.6124=The valid AWS Cloud Type is government or commercial.
- error.code.6125=Failed update AWS Access credentials. Please contact your Administrator.
- error.code.6126=Failed verify AWS Access credentials. Please contact your Administrator.
- error.code.6130=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.6131=Attempted to create resources beyond the current AWS account limits. Please contact your system administrator.
- error.code.6132=AWS Key Pair can be changed only by random generation.
- error.code.6201=AWS Master Account Name is an email address.
- error.code.6280=Invalid or missing port number.
- error.code.6301=Domain not specified.
- error.code.6302=Invalid port number.
- error.code.6303=Login account not found. Check login info specified in `nisConnector.properties`.
- error.code.6311=Failed to connect to host.
- error.code.6312=Failed to initialize change password process.
- error.code.6313=Password update failed.
- error.code.6314=Password verify failed.
- error.code.6315=Failed to load `nisConnector.properties` file.
- error.code.6316=Invalid Verify Timeout specified in `nisConnector.properties` file.
- error.code.6317=Invalid Update Timeout specified in `nisConnector.properties` file.

- error.code.6401=Invalid port specified.
- error.code.6402=Realm not specified.
- error.code.6403=Change process not specified.
- error.code.6410=Failed to synchronize/verify account. See logs for details.
- error.code.6411=Invalid account specified.
- error.code.6412=Failed to connect to host.
- error.code.6413=Invalid Realm specified.
- error.code.6414=Failed to synchronize/verify account. Login failed.
- error.code.6450=Invalid or missing port number.
- error.code.6451=Change process not specified.
- error.code.6452=Invalid value specified for the `disableAutoConnectTargetAccount` parameter.
- error.code.6470=Cannot connect to ESX/ESXi host.
- error.code.6471=Invalid login, username or password is incorrect.
- error.code.6472=No permission to update credentials.
- error.code.6473=User not found.
- error.code.6474=Remote system error.
- error.code.6475=Invalid request.
- error.code.6476=User not authenticated.
- error.code.6477=Remote security error.
- error.code.6500=An SSH port number must be specified.
- error.code.6501=A connection timeout must be specified.
- error.code.6502=A read timeout must be specified.
- error.code.6503=Invalid change process specified.
- error.code.6504=An invalid connection timeout value was specified.
- error.code.6505=An invalid read timeout value was specified.
- error.code.6506=An invalid SSH port number was specified.
- error.code.6525=Failed to verify account.
- error.code.6526=Failed to update account.
- error.code.6527=An unknown error occurred; please consult the server log or contact your Administrator.
- error.code.6528=User not found.
- error.code.6529=Failed to update password; the target device is currently in use by another user.
- error.code.6530=Failed to connect to the target device; a timeout occurred while waiting to connect.
- error.code.6531=Failed to authenticate to the target device due to invalid credentials.
- error.code.6532=A communications error occurred while receiving data from the target device.
- error.code.6533=User has insufficient permissions.
- error.code.6551=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.6552=Failed to load the default or revised update script file.
- error.code.6553=Failed to load the default or revised verify script file.
- error.code.6554=Failed to update account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6555=Failed to verify account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6580=An invalid SSH port number was specified; the value must be in the range 0.65535.



- error.code.6600=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.6601=Failed to load the default or revised update script file.
- error.code.6602=Failed to load the default or revised verify script file.
- error.code.6603=Failed to enter privilege mode. Review the log file for further information or else contact your Administrator.
- error.code.6604=Failed to update account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6605=Failed to enter configuration mode. Please try again. If problem persist contact your Administrator.
- error.code.6606=Failed to verify account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6630=An invalid SSH port number was specified; the value must be in the range 0.65535.
- error.code.6660=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.6670=Failed update AWS account credentials. Please contact your Administrator.
- error.code.6671=Failed verify AWS account credentials. Please contact your Administrator.
- error.code.6672=Password did not meet the requirements imposed by the account password policy. Please contact your Administrator.
- error.code.6673=Account is temporarily unmodifiable. Please try again after waiting several minutes or contact your Administrator.
- error.code.6674=Current account does not exist. Please contact your Administrator.
- error.code.6675=Trying to create resources beyond the current AWS account limits. Please contact your Administrator.
- error.code.6680=AWS Access Account must be specified.
- error.code.6700=An unknown error occurred. Review the log file for further information or else contact your Administrator.
- error.code.6701=Failed to load the default or revised update script file.
- error.code.6702=Failed to load the default or revised verify script file.
- error.code.6703=Failed to update account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6704=Failed to verify account credentials. Review the log file for further information or else contact your Administrator.
- error.code.6705=Cannot verify account's credentials for non Privilege account type; the operation is not supported.
- error.code.6706=Cannot update account's credentials for non Privilege account type; the operation is not supported.
- error.code.6707=Cannot change password. Please enter a password with 1 to 15 characters.
- error.code.6720=An invalid SSH port number was specified; the value must be in the range 0.65535.
- error.code.6721=An invalid SSH communication timeout was specified; the value must be in the range 1000.99999.
- error.code.6722=An invalid script processor read timeout was specified; the value must be in the range 1000.59999.
- error.code.6723=The value assigned to the 'useUpdateScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.
- error.code.6724=The value assigned to the 'useVerifyScriptType ' attribute must be 'DEFAULT', 'REVISED' or 'REPLACEMENT'.



- error.code.8001=LDAP authentication module configuration error.
- error.code.8002=LDAP authentication module configuration error.
- error.code.8003=LDAP authentication module configuration error.
- error.code.8004=LDAP authentication module configuration error.
- error.code.8005=LDAP authentication module configuration error.
- error.code.8006=Failed to connect to LDAP server.
- error.code.8007=LDAP authentication module commit error.
- error.code.8008=LDAP authentication failed.
- error.code.8009=LDAP authentication failed.
- error.code.8201=Kerberos authentication module configuration error.
- error.code.8202=Kerberos authentication module error - clock skew too great.
- error.code.8203=Kerberos authentication module error - Communication Timeout.
- error.code.8204=Kerberos authentication module configuration error.
- error.code.8205=Kerberos authentication module configuration error.
- error.code.8301=X509 authentication module invalid credentials.
- error.code.8302=X509 authentication module error - expired certificate.
- error.code.8303=X509 authentication module error - certificate not yet valid.
- error.code.8304=X509 authentication module error - certificate revoked.
- error.code.8305=X509 authentication module error - root CA invalid.
- error.code.8306=X509 authentication module error - invalid certificate signature.
- error.code.8307=X509 authentication module error - invalid configuration.
- error.code.8308=X509 authentication module error - invalid certificate store file.
- error.code.8309=X509 authentication module error - invalid certificate store.
- error.code.8310=X509 authentication module error - invalid LDAP port.
- error.code.8311=X509 authentication module error - invalid LDAP certificate store.
- error.code.8401=X509 LDAP authentication module invalid credentials.
- error.code.8402=X509 LDAP authentication module error - expired certificate.
- error.code.8403=X509 LDAP authentication module error - certificate not yet valid.
- error.code.8404=X509 LDAP authentication module error - certificate revoked.
- error.code.8405=X509 LDAP authentication module error - root CA invalid.
- error.code.8406=X509 LDAP authentication module error - invalid certificate signature.
- error.code.8407=X509 LDAP authentication module error - invalid configuration.
- error.code.8408=X509 LDAP authentication module error - invalid certificate store file.
- error.code.8409=X509 LDAP authentication module error - invalid certificate store.
- error.code.8410=X509 LDAP authentication module error - invalid LDAP port.
- error.code.8411=X509 LDAP authentication module error - invalid LDAP certificate store.
- error.code.8501=Active Directory authentication module configuration error.
- error.code.8502=Active Directory authentication module configuration error.
- error.code.8503=Active Directory authentication module configuration error.
- error.code.8504=Active Directory authentication module configuration error.
- error.code.8505=Active Directory authentication module configuration error.
- error.code.8506=Failed to connect to Active Directory Server.

- error.code.10001=Failed to log into the LunaSA Module.
- error.code.10002=Failed to retrieve key from LunaSA Module.
- error.code.10003=Failed to persist key in LunaSA Module.
- error.code.10004=Failed to generate key in LunaSA Module.
- error.code.10101=Failed to login to the LunaSA Module.
- error.code.10102=Failed to retrieve key from LunaSA Module.
- error.code.10103=Failed to persist key in LunaSA Module.
- error.code.10104=Failed to generate key in LunaSA Module.
- error.code.10201=Failed to log into the LunaSA Module.
- error.code.10202=Failed to retrieve key from LunaSA Module.
- error.code.10203=Failed to persist key in LunaSA Module.
- error.code.10204=Failed to generate key in LunaSA Module.
- error.code.12000=targetServerHostName property not found in authorization.xml.
- error.code.12001=Target Server named in authorization.xml not found in Password Authority.
- error.code.12002=targetApplication property not found in authorization.xml.
- error.code.12003=Target Application named in authorization.xml not found in Password Authority.
- error.code.12004=targetAccount property not found in authorization.xml.
- error.code.12005=Target Account named in authorization.xml not found in Password Authority.
- error.code.12006=groupClassMemberList property not found in authorization.xml.
- error.code.12007=userSearchFilter property not found in authorization.xml.
- error.code.12050=Error communicating with the LDAP server.
- error.code.12051=Error authenticating with the LDAP server.
- error.code.12052=Target account/application in authorization.xml file must be of type LDAP or Windows Domain Service.
- error.code.12053=Cannot retrieve DNS host name(s).
- error.code.12054=DNS server name not specified.
- error.code.12100=targetServerHostName property not found in authorization.xml.
- error.code.12101=Target Server named in authorization.xml not found in Password Authority.
- error.code.12102=targetApplication property not found in authorization.xml.
- error.code.12103=Target Application named in authorization.xml not found in Password Authority.
- error.code.12104=targetAccount property not found in authorization.xml.
- error.code.12105=Target Account named in authorization.xml not found in Password Authority.
- error.code.12106=userSearchFilter property not found in authorization.xml.
- error.code.12107=Error communicating with the Active Directory Server.
- error.code.12108=Error authenticating with the Active Directory Server.

**Error Code Messages for Remedy View Password Plug-in (13000 - 13099)**

- error.code.13000=A Remedy server must be specified.
- error.code.13001=A Remedy application must be specified.
- error.code.13002=A Remedy account must be specified.
- error.code.13003=Remedy ticket number is not specified, or incorrect.
- error.code.13004=Could not log into Remedy server.
- error.code.13005=Remedy server specified in the password view policy could not be found.
- error.code.13006=Remedy application specified in the password view policy could not be found.
- error.code.13007=Remedy account specified in the password view policy could not be found.
- error.code.13008=The CA NIM SM target server could not be found.
- error.code.13009=The CA NIM SM target application could not be found.
- error.code.13010=The CA NIM SM target account could not be found.
- error.code.13011=Could not retrieve the ticket from the Remedy system.
- error.code.13012=Required Remedy licensed files could not be found.
- **Error Code Messages for ServiceNow View Password Plug-in (13100 - 13199)**
- error.code.13100=A ServiceNow server must be specified.
- error.code.13101=A ServiceNow application must be specified.
- error.code.13102=A ServiceNow account must be specified.
- error.code.13103=ServiceNow ticket number is not specified, or incorrect.
- error.code.13104=Could not log into ServiceNow server.
- error.code.13105=ServiceNow server specified in the password view policy could not be found.
- error.code.13106=ServiceNow application specified in the password view policy could not be found.
- error.code.13107=ServiceNow account specified in the password view policy could not be found.
- error.code.13108=The CA NIM SM target server could not be found.
- error.code.13109=The CA NIM SM target application could not be found.
- error.code.13110=The CA NIM SM target account could not be found.
- error.code.13111=Could not retrieve the ticket from the ServiceNow system.

***Error Code Messages for CA SDM View Password Plug-in (13200 - 13299)***

- error.code.13200=A CA SDM server must be specified.
- error.code.13201=A CA SDM application (type: Generic) must be specified.
- error.code.13202=A CA SDM account must be specified.
- error.code.13207=CA SDM ticket number is not specified, or incorrect.
- error.code.13208=Could not log into CA SDM server.
- error.code.13209=CA SDM server specified in the password view policy could not be found.
- error.code.13210=CA SDM application specified in the password view policy could not be found.
- error.code.13211=CA SDM account specified in the password view policy could not be found.
- error.code.13212=The CA NIM SM target server could not be found.
- error.code.13213=The CA NIM SM target application could not be found.
- error.code.13214=The CA NIM SM target account could not be found.
- error.code.13215=Could not retrieve the ticket from the CA SDM system.

***Error Code Messages for Salesforce Service Cloud View Password Plug-in (13400 - 13499)***

- error.code.13400=A Salesforce Service Cloud server must be specified.
- error.code.13401=A Salesforce Service Cloud application (type: Generic) must be specified.
- error.code.13402=A Salesforce Service Cloud account must be specified.
- error.code.13403=An SFDC Login Endpoint must be specified.
- error.code.13404=An SFDC Service Cloud Client URL must be specified.
- error.code.13405=A `DateFormat` must be specified.
- error.code.13406=A `CaseObject` must be specified.
- error.code.13407=A `CaseCommentObject` must be specified.
- error.code.13408=An `AttachmentObject` must be specified.
- error.code.13409=Salesforce Service Cloud ticket number is not specified, or incorrect.
- error.code.13410=Could not log into Salesforce Service Cloud server.
- error.code.13411=Salesforce Service Cloud server specified in the password view policy could not be found.
- error.code.13412=Salesforce Service Cloud application specified in the password view policy could not be found.
- error.code.13413=Salesforce Service Cloud account specified in the password view policy could not be found.
- error.code.13414=The CA NIM SM target server could not be found.
- error.code.13415=The CA NIM SM target application could not be found.
- error.code.13416=The CA NIM SM target account could not be found.
- error.code.13417=Could not retrieve the ticket from the Salesforce Service Cloud system.

**Error Code Messages for HP Service Manager View Password Plug-in (13500 - 13599)**

- error.code.13500=An HP Service Manager server must be specified.
- error.code.13501=An HP Service Manager application (type: Generic) must be specified.
- error.code.13502=An HP Service Manager account must be specified.
- error.code.13506=HP Service Manager ticket number is not specified, or incorrect.
- error.code.13507=Could not log into HP Service Manager server.
- error.code.13508=HP Service Manager server specified in the password view policy could not be found.
- error.code.13509=HP Service Manager application specified in the password view policy could not be found.
- error.code.13510=HP Service Manager account specified in the password view policy could not be found.
- error.code.13511=The CA NIM SM target server could not be found.
- error.code.13512=The CA NIM SM target application could not be found.
- error.code.13513=The CA NIM SM target account could not be found.
- error.code.13514=Could not retrieve the ticket from the HP Service Manager system.

**Custom View Password Module Error Code Messages (14000 - 14999)**

- error.code.14000=The specified CA Normalized Integration Management account is in use and can't be deleted.
- error.code.14001=The requested operation is not allowed on the CA Normalized Integration Management Target Account.
- error.code.14002=The requested operation is not allowed on the CA Normalized Integration Management Target Application.
- error.code.14003=The requested operation is not allowed on the '[nim.pam.ca.com](http://nim.pam.ca.com)' Target Server.
- error.code.14004=The requested operation is not allowed on the selected application type.
- error.code.15000=An invalid issuer URL was specified.
- error.code.15001=An invalid console URL was specified.
- error.code.15002=An invalid sign-in URL was specified.
- error.code.15003=Exceeded maximum length for URL parameter.
- error.code.15004=The specified URL is not formatted correctly.
- error.code.15005=An invalid session duration was specified; the allowed range is 3600 - 129600 seconds.
- error.code.15006=An invalid policy was specified.
- error.code.15007=Exceeded maximum length for policy parameter.
- error.code.15008=The specified policy is not formatted correctly.
- error.code.15009=The AWS client reports that corrupted data was received from the AWS server; the error message is: {0}
- error.code.15010=The AWS client reports that communications with the AWS server failed; the error message is: {0}
- error.code.15011=An invalid session URL encoding option was specified.
- error.code.15012=The AWS service reported a problem; the error message is: {0}
- error.code.15013=The requested operation is not allowed on the AWS Access Credentials Target Application.
- error.code.15014=The requested operation is not allowed on the '[xceedium.aws.amazon.com](http://xceedium.aws.amazon.com)' Target Server.
- error.code.15015=The requested command cannot be invoked from a remote host.
- error.code.15016=The specified federated user name is incompatible with AWS; it contains too few characters.
- error.code.15017=The specified federated user name is incompatible with AWS; it contains too many characters.
- error.code.15018=The federated user name is missing from the request.
- error.code.15019=The specified federated user name is incompatible with AWS.
- error.code.15020=The specified AWS access account is in use and can't be deleted.
- error.code.15021=The requested operation is not allowed on the AWS API Proxy Credentials Target Account.
- error.code.15022=The requested operation cannot be performed by user with the specified target application type.
- error.code.15023=The requested operation is not allowed
- error.code.15099=The specified VMware access account is in use and can't be deleted.
- error.code.15100=Delete Check: the requested operation would delete an existing Target Server with ID: {0}
- error.code.15101=Delete Check: the specified host name corresponds to one or more deleted Target Server(s): {0}
- error.code.15102=Delete Check: the specified host name does not correspond to any existing or deleted Target Server(s): {0}
- error.code.15103=Delete Check: the specified ID corresponds to a deleted Target Server: {0}
- error.code.15104=Delete Check: the specified ID does not correspond to an existing or deleted Target Server: {0}
- error.code.15105=Delete Check: the requested operation would delete an existing Request Server of type CLIENT or AGENT with ID: {0}
- error.code.15106=Delete Check: the specified host name corresponds to one or more deleted Request Server(s) of type {1}: {0}
- error.code.15107=Delete Check: the specified host name does not correspond to any existing or deleted Request Server(s) of type {1}: {0}
- error.code.15108=Delete Check: the specified ID corresponds to a deleted Request Server of type CLIENT or AGENT: {0}
- error.code.15109=Delete Check: the specified ID does not correspond to an existing or deleted Request Server of type CLIENT or AGENT: {0}
- ~~error.code.15110=Delete Check: the specified ID corresponds to one or more deleted Target Server(s): {0}~~
- error.code.15111=Delete Check: the specified ID does not correspond to any existing or deleted Target Server(s): {0}

**Extension Manager: Common Channel and Processor Target Connector API (15200 - 15299)**

- error.code.15200=Failed to process a target connector script. Refer to the log file for further information.
- error.code.15201=Failed to store an object in script processor memory.
- error.code.15202=Failed to retrieve an object from storage in script processor memory.
- error.code.15203=Failed to reset the script processor.
- error.code.15204=An error occurred while processing a target connector script. The Target Account specifies an unrecognized password change method.
- error.code.15205=An error occurred while processing a target connector script. The Target Account specifies an unsupported protocol.
- error.code.15206=An error occurred while configuring the communications channel. The Target Account specifies an unsupported protocol.
- error.code.15207=Failed to find {0} pattern(s) while reading from the communications channel: {1}
- error.code.15208=An error occurred while configuring the script processor. Failed to retrieve a Target Account with ID {0}.
- error.code.15209=An error occurred while configuring the script processor. The Target Account specifies another account should be used for authentication and/or verification but no value is assigned to the other account attribute.
- error.code.15210=An error occurred while configuring the communications channel. The specified and calculated known host key fingerprints do not match.
- error.code.15211=An error occurred while configuring the communications channel. Failed to decode the known host key.
- error.code.15212=Failed to establish a communications channel to the remote host.
- error.code.15213=An error occurred while configuring the script processor. An invalid pattern was specified for the password entry prompt.
- error.code.15214=An error occurred while configuring the script processor. An invalid pattern was specified for the password confirmation prompt.
- error.code.15215=An error occurred while configuring the script processor. An invalid pattern was specified for the password change prompt.
- error.code.15216=An error occurred while configuring the script processor. An invalid pattern was specified for the user name entry prompt.
- error.code.15217=Failed to remove an object from storage in script processor memory.
- error.code.15218=An error occurred while configuring the script processor. Failed to retrieve a Target Account with ID {0}.
- error.code.15219=An error occurred while configuring the script processor. The Target Account specifies another privileged account should be used but no value is assigned to the other privileged account attribute.
- error.code.15220=A problem occurred while executing the script processor. Please try your request again or contact your Administrator.
- error.code.15221=A problem occurred while executing the script processor. Failed to automatically derive a public key. Specify the public key and try again or else contact your Administrator.

**Extension Manager: Common Channel and Processor Target Connector UI (15300 - 15399)**

- error.code.15300=Cannot read the revised update script file. Verify the filename and ensure the patch obtained from Customer Support has been applied.
- error.code.15301=Cannot read the revised verify script file. Verify the filename and ensure the patch obtained from Customer Support has been applied.
- error.code.15302=An invalid filename was specified for the revised update script file. Verify the filename or else contact Customer Support to obtain the correct filename.
- error.code.15303=An invalid filename was specified for the revised verify script file. Verify the filename or else contact Customer Support to obtain the correct filename.
- error.code.15304=Must choose the filename of the revised update script if any are available. Only use this field if instructed to do so by Customer Support.
- error.code.15305=Must choose the filename of the revised verify script if any are available. Only use this field if instructed to do so by Customer Support.
- error.code.15306=An invalid regular expression was specified to match the Password Change prompt.
- error.code.15307=An invalid list of server host key types was specified.
- error.code.15308=An invalid list of inbound compression methods was specified.
- error.code.15309=An invalid list of key exchange algorithms was specified.
- error.code.15310=An invalid list of outbound compression methods was specified.
- error.code.15311=An invalid list of inbound hashes was specified.
- error.code.15312=An invalid list of outbound hashes was specified.
- error.code.15313=An invalid list of inbound ciphers was specified.
- error.code.15314=An invalid list of outbound ciphers was specified.
- error.code.15315=Must specify a replacement update script. Only use this field if instructed to do so by Customer Support.
- error.code.15316=Must specify a replacement verify script. Only use this field if instructed to do so by Customer Support.
- error.code.15317=An invalid list of ciphers to detect was specified.
- error.code.15318=An invalid regular expression was specified to match the Password Confirmation prompt.
- error.code.15319=An invalid regular expression was specified to match the Password Entry prompt.
- error.code.15320=An invalid regular expression was specified to match the User Name Entry prompt.

**Error Messages for Microsoft Office 365 (Online Portal) (15400 - 15499)**



- error.code.15400=The portal URL is missing from the request.
- error.code.15401=The specified portal URL is invalid.
- error.code.15402=The Security Token Service endpoint URL is missing from the request.
- error.code.15403=The specified Security Token Service endpoint URL is invalid.
- error.code.15404=The Security Token Service endpoint reference URI is missing from the request.
- error.code.15405=The specified Security Token Service endpoint reference URI is invalid.
- error.code.15408=The context (`wctx`) parameter is missing from the request.
- error.code.15409=The specified context (`wctx`) parameter is invalid.
- error.code.15410=Failed to load the token request template.
- error.code.15411=Failed to initiate federated session.
- error.code.15412=Failed to retrieve token request response from the Security Token Service.
- error.code.15413=Failed to load the federated session request template.
- error.code.15414=Failed to retrieve target account password.
- error.code.15415=The target account ID is missing from the request.
- error.code.15416=The specified target account ID is invalid.
- error.code.15419=The reason parameter is missing from the request.
- error.code.15421=The specified start date is invalid.
- error.code.15423=The specified end date is invalid.
- error.code.15424=The specified compound server ID is invalid.
- error.code.15425=Failed to encode the specified context (`wctx`) parameter.

#### **Error Messages for SSH Key Pair Policy (15500 - 15599)**

- error.code.15500=The SSH Key Pair Policy ID is missing.
- error.code.15501=The specified SSH Key Pair Policy ID is invalid; it must be an integer greater than zero.
- error.code.15502=The SSH Key Pair Policy name is missing.
- error.code.15503=The specified SSH Key Pair Policy name is invalid; it must consist of characters [a-z, A-Z, 0-9].
- error.code.15504=The specified SSH Key Pair Policy name is too long; reduce the number of characters that it contains.
- error.code.15505=The SSH Key Pair Policy description is missing.
- error.code.15506=The SSH Key Pair Policy description is invalid; it must consist of characters [a-z, A-Z, 0-9].
- error.code.15507=The SSH Key Pair Policy description is too long; reduce the number of characters that it contains.
- error.code.15508=The SSH Key Pair Policy key type is missing.
- error.code.15509=The specified SSH Key Pair Policy key type is invalid; it must be ECDSA or RSA or DSA.
- error.code.15510=The SSH Key Pair Policy key length is missing.
- error.code.15511=The specified SSH Key Pair Policy key length is invalid.
- error.code.15512=Failed to add SSH Key Pair Policy due to error: {0}
- error.code.15513=Failed SSH Key Pair generation test due to error: {0}
- error.code.15514=The specified SSH Key Pair type and length are not compatible.
- error.code.15515=An SSH Key Pair Policy ID or Name must be specified.
- error.code.15516=Failed to load an SSH Key Pair Policy having the specified ID or Name.
- error.code.15517=Must specify either an SSH Key Pair Policy ID or a Name but not both.
- error.code.15600=Invalid subnet x.x.x.x. Format should be in CIDR notation (xxx.xxx.xxx.xxx/xx)



- error.code.15601=Cannot change host name. Device in use by LDAP Domain Configuration.
- error.code.15602=Cannot change host name. Application in use by LDAP Domain Configuration.
- error.code.15603=Cannot change application. Account in use by LDAP Domain Configuration.
- error.code.15604=Failure updating LDAP configuration
- error.code.15605=Cannot change host name. Device in use by RADIUS and TACACS+ Configuration.
- error.code.15606=Cannot change application type. Application in use by RADIUS and TACACS+ Configuration.
- error.code.15607=Cannot change application. Account in use by RADIUS and TACACS+ Configuration.

**Remote Agent Error Codes (15608 - 15622)**

- error.code.15608=Remote Agent other account
- error.code.15609=Cannot change application. Account in use by another Windows Remote Agent account.
- error.code.15610=Cannot change account type. Account in use by another Windows Remote Agent account.
- error.code.15611=Cannot change application. Account in use for discovery by an Active Directory account.
- error.code.15612=Cannot change account type. Account in use for discovery by an Active Directory account.
- error.code.15613=Not a Remote Agent admin
- error.code.15614=Remote Agent I/O error
- error.code.15615=Remote Agent process interrupted
- error.code.15616=Remote Agent process abnormal exit
- error.code.15617=Remote Agent logon failed
- error.code.15618=Remote Agent access denied
- error.code.15619=Remote Agent connection error
- error.code.15620=No Remote Agent admin
- error.code.15621=Remote Agent cannot clean up
- error.code.15622=No Remote Agent admin ID
- error.code.15623=Account is in use by Azure Configuration.
- error.code.15624=Operation is not permitted on Azure access credentials target server

**Error messages for CA NIM SM target manager connector (15700 - 15719)**

- error.code.15701=Change process not specified.
- error.code.15702=Internal target connector error.
- error.code.15703=Failed to synchronize password with target.
- error.code.15704=Failed to verify password with target.

**Error Code Messages for CA NIM UM Target Manager Connector (15720 - 15739)**

- error.code.15721=Change process not specified.
- error.code.15722=Internal target connector error.
- error.code.15723=Failed to synchronize password with target.
- error.code.15724=Failed to verify password with target.

**Error Code Messages for ServiceNow Target Manager Connector (15740 - 15759)**

- error.code.15741=Change process not specified.
- error.code.15742=Internal target connector error.
- error.code.15743=Failed to synchronize password with target.
- error.code.15744=Failed to verify password with target.
- error.code.15745=A ServiceNow URL must be specified.
- error.code.15746=A `ServiceNowClientURL` must be specified.
- error.code.15747=Could not log into ServiceNow server.

**Basic error messages for Service Desk connector (15760 - 15779)**

- error.code.15760=Error retrieving Service Desk user credentials.
- error.code.15761=The CA NIM UM target server could not be found.
- error.code.15762=The CA NIM UM target application specified in the password view policy could not be found.
- error.code.15763=The CA NIM UM target account specified in the password view policy could not be found.
- error.code.15764=Failed to synchronize password with target.
- error.code.15765=Failed to verify password with target.

***Error messages for HP Service Manager target manager connector (15780 - 15799)***

- error.code.15780=Change process not specified.
- error.code.15781=Internal target connector error.
- error.code.15782=Failed to synchronize password with target.
- error.code.15783=Failed to verify password with target.
- error.code.15784=A port must be specified.
- error.code.15785=A `HPSMClientURL` must be specified.
- error.code.15786=An Enabled Protocol must be specified.
- error.code.15787=Could not log into HP Service Manager server.

***Error Code Messages for CA SDM Target Manager Connector (15800 - 15819)***

- error.code.15800=Change process not specified.
- error.code.15801=Internal target connector error.
- error.code.15802=SOAP Protocol must be specified.
- error.code.15803=SOAP Port must be specified.
- error.code.15804=REST Protocol must be specified.
- error.code.15805=REST Port must be specified.
- error.code.15806=Could not log into CA SDM server.

***SSH Certificate Policy Error Messages***

- error.code.18000=The SSH Certificate Policy ID is missing.
- error.code.18001=The specified SSH Certificate Policy ID is invalid; it must be an integer greater than zero.
- error.code.18002=The SSH Certificate Policy name is missing.
- error.code.18003=The specified SSH Certificate Policy name is invalid; it must consist of characters [a-z, A-Z, 0-9].
- error.code.18004=The specified SSH Certificate Policy name is too long; reduce the number of characters that it contains.
- error.code.18005=The SSH Certificate Policy description is missing.
- error.code.18006=The SSH Certificate Policy description is invalid; it must consist of characters [a-z, A-Z, 0-9].
- error.code.18007=The SSH Certificate Policy description is too long; reduce the number of characters that it contains.
- error.code.18008=The SSH Certificate Policy force command is too long; reduce the number of characters that it contains.
- error.code.18009=The specified SSH Certificate Policy permit-x11-forwarding is invalid; it must be true or false.
- error.code.18010=The specified SSH Certificate Policy permit-pty is invalid; it must be true or false.
- error.code.18011=The specified SSH Certificate Policy permit-port-forwarding is invalid; it must be true or false.
- error.code.18012=The specified SSH Certificate Policy permit-user-rc is invalid; it must be true or false.
- error.code.18013=An SSH Certificate Policy ID or Name must be specified.
- error.code.18014=Failed to load an SSH Certificate Policy having the specified ID or Name.
- error.code.18015=Must specify either an SSH Certificate Policy ID or a Name but not both.
- error.code.18016=Failed to add an SSH Certificate Policy having the specified ID or Name.
- error.code.18017=The SSH Certificate Policy permit-x11-forwarding is missing.
- error.code.18018=The SSH Certificate Policy permit-pty is missing.
- error.code.18019=The SSH Certificate Policy permit-port-forwarding is missing.
- error.code.18020=The SSH Certificate Policy permit-user-rc is missing.
- error.code.18021=Cannot delete Default policy.
- error.code.18022=Cannot update Default policy's name.

## Credential Manager Terms and Concepts

The following terms and concepts are used regarding Credential Manager.

- **Application-to-application (A2A) accounts:** A2A accounts are accessed by applications in addition to users. For example, database accounts are used by web pages to retrieve information from the database.
- **Batch processing:** The Credential Manager CLI feature that lets you read an XML formatted file as input to a registration activity.
- **Credentials:** User name and password or RSA key that is associated with an account
- **Master account:** A target account that is used to change another account. This account must have the ability to change another account password, such as `root` or `sudo` -enabled accounts in UNIX. See also Slave account.
- **Privileged accounts:** Accounts that have elevated privileges; for example, UNIX root accounts and database administrator accounts. Attended privileged accounts are associated with people. Unattended privileged accounts are associated with automated applications or machines. Privileged accounts can usually affect multiple users. Privileged accounts are often used for access and password viewing. See also Unprivileged accounts.
- **Remote account:** An account on or accessible by a remote host. Some accounts can be considered to be on multiple hosts. For example, an account is stored in a directory, such as AD or LDAP. The account can be managed in the directory server or on a remote host when the account is typically used, such as a user desktop. There can be multiple

target application types that manage a given remote account although typically not. This situation usually occurs for Windows accounts or account in a directory server.

- **Remote application:** An application on a remote host, such as the OS or a Database Management System (DBMS)
- **Remote host:** A computing platform other than the Privileged Access Manager appliance. Examples include servers, laptops, desktops, and routers.
- **Roles:** A collection of actions that can be performed on the GUI and CLI. Roles can be built for each series of permissions you want to assign to Credential Manager administrators. Credential Manager roles are distinct and separate from Privileged Access Manager roles. See [Credential Manager Group Terminology](#).
- **Slave account:** A target account whose password is changed by a master account. See also Master account.
- **Synchronized credentials:** The ability of Credential Manager to renew credentials on target applications using a predetermined process to keep the Privileged Access Manager appliance and requestor synchronized.
- **Target:** General term for a target account, target application, and target server.
- **Target account:** An account that is located on a remote host and is managed by Credential Manager.
- **Target applications:** Applications on a remote host that require credentials for access. Examples include a databases or the remote host OS. A target application can contain one or more target accounts. Multiple target application types exist, each corresponding to a different target connector.
- **Target connector:** Code and extensions that are applied to the Credential Manager target application and target account details pages that communicate with a given type of remote application. Each target connector is associated with a target application.
- **Target group:** A collection of target servers, target applications, or target accounts that meet specific filter criteria; for example, all target servers that have the identifier `London` in the descriptor field. A single target can belong to multiple target groups. When a target group consists of target servers, all applications and accounts on that server are automatically within that target group.
- **Target server:** A server hosting one or more target applications. In the *Privileged Access Manager* appliance, it is configured as a Device of type **Password Management**.
- **Unprivileged accounts:** Accounts that have restricted privileges, usually allowing a user to read or affect only their own data. See also privileged accounts. See also Privileged accounts.
- **User group:** A collection of one target group, one requestor group, and one role. Credential Manager user groups are distinct and separate from Privileged Access Manager User Groups. See [Credential Manager Group Terminology](#).
- **Users:** Users are people that access and operate Credential Manager. Each user belongs to one or more user groups. The user groups define what targets and requestors the user can see and what actions the user can perform on the Credential Manager interfaces.

## **A2A Terminology**

In addition, the following terms and concepts apply when referring to Application-to-application (A2A) functionality:

- **Client:** A program that identifies information about the invoking program or script (such as its name, path, hash, and `userId`). For UNIX and Linux, the client stub is `cspmclient`. For Windows, the client stub is `cspmclient.exe`. For Java programs, the client stub is `cspmclient.jar`.
- **Client daemon or service:** A UNIX daemon or Windows service that caches credentials from the Privileged Access Manager appliance. The A2A Client requests credentials from it. If the credentials are not cached, it requests the credentials from the Privileged Access Manager appliance. It then caches them before returning the credentials to the client.
- **Requestor application:** Applications that initiate communications with target applications using target credentials. Requestor applications invoke a client stub to communicate to the Privileged Access Manager appliance to get the required credentials.
- **Requestor group:** A collection of requestors or requestor servers that meet specific filter criteria; for example, all requestor servers that have the identifier `London` in the descriptor field. A single requestor can belong to

multiple requestor groups. When a requestor group consists of requestor servers, all requestors on that server are automatically within that requestor group.

- **Requestor script:** A Perl, Python, PHP, sh, ksh, or csh script that invokes a client stub to get credentials.
- **Requestor server:** A server hosting one or more requestors

## Windows Shortcut Keys for the RDP Client

The following table lists the shortcut keys for the Privileged Access Manager RDP Client and their comparison to standard shortcut keys supported by native Windows RDP Client (mstsc):

Key	Action	Mstsc (non full screen mode)	Mstsc (full screen mode)	PAM RDP Client
Alt+Delete	Opens the Windows menu.	Yes	No	The Content Menu appears
Alt+Esc	Cycles through programs in the order that they were started.	No	Yes	No
Alt+Home	Opens the Start menu.	Yes	No	Yes
Alt+Insert	Cycles through programs in the order that they were started.	Yes	No	Yes
Alt+Page Down	Switches between programs from right to left.	Yes	No	Yes
Alt+Page Up	Switches between programs from left to right.	Yes	No	Yes
Alt+Shift+Home	Opens the Task Manager	Yes	No	Yes
Alt+Space	Opens the Windows menu.	No	Yes	No
Alt+Tab	Switches between programs from left to right.	No	Yes	No
Ctrl+Alt+Break	Switches the client between full-screen mode and window mode.	Yes	Yes	No
Ctrl+Alt+Minus Sign (-)	Places a snapshot of the active window, within the client, on the Remote Desktop Session Host (RD Session Host) server Clipboard. This provides the same functionality as pressing Alt+Print Screen on the local computer.	Yes	No	No
Ctrl+Alt+Plus Sign (+)	Places a snapshot of the entire client windows area on the RD Session Host server Clipboard. This provides the same functionality as pressing	Yes	No	No

	PRINT SCREEN on the local computer.			
Ctrl+Break	Breaks the execution of a console application.	Yes	Yes	No
Ctrl+Esc	Opens the Start menu.	No	Yes	No
Ctrl+Shift+Esc	Opens the Task Manager	No	Yes	No

In addition, the Privileged Access Manager RDP Client handles this key combination in the following way:

Key	Action
Alt+Enter	Switch to full screen mode.

## Upgrade

These general instructions describe the function of the Upgrade page on the product UI. For upgrade instructions pertaining to specific upgrades, patches, or hotfixes, see the Upgrading section for that version on [Techdocs](#).

### **Backup and Recovery**

Backup and Recovery is offered as a precaution you take before upgrading your appliance. The Backup and Recovery tab functions only on a physical appliance.

- For virtual machines, take a "snapshot" using a product such as VMware vSphere.
- See [AWS AMI Backup and Recovery](#) for backup and recovery information for AWS instances.

### **Perform Full Appliance Backup**

This button provides a full system backup, including OS, firmware, configuration settings of the appliance, and the provisioning data of managed users and devices. The backup is saved to the appliance internal secondary drive. Note these characteristics of system backups:

- Only a single backup is maintained. Because the secondary drive stores up to an entire primary drive capacity, it can contain only the most recently executed Backup.
- Upgrades automatically back up the appliance. As part of any upgrade, or any hotfix that requires a reboot, Privileged Access Manager performs the backup process automatically and silently.
- A full copy is made. During the backup process, the secondary drive makes a complete copy of the primary drive.
- The product reboots automatically. After it copies the primary drive, the appliance will automatically reboot.

### **Recover Appliance from Latest Backup**

Perform recovery only with the assistance of CA Support.

A Privileged Access Manager backup on the internal secondary drive can be restored by clicking the Recover button. If the system has become inaccessible from the network, Recover is also possible from the Console.

### **NOTE**

Patch binaries use HMAC (Hash-based Message Authentication Code), a FIPS 140-2 requirement, and SHA 256. Privileged Access Manager verifies HMAC-SHA-256 on all appliances (FIPS or not). Upgrade patches and diagnostic patches that are supplied by Broadcom Support are all included.

### **Upgrade**

1. Navigate to **Configuration, Upgrade**.

2. In the **Upgrade History** section, confirm that your currently installed upgrades include all necessary patches to enable upgrade to the current release.
3. Select **Choose File** and select the upgrade file in the file browser. Do not select the payload file.
4. Select **Upload And Apply**. The UI and the LCD display show messages as the upgrade progresses. These messages might display for several minutes.

**Important!** Keep your browser open until you see the final reboot message. Do not interrupt the upgrade process.

5. Optionally, select **Show Checksums**. This option recomputes the downloaded file's checksum value to verify that the file was not corrupted during the upload process. Compare this newly generated value with the value of the checksum file included in the downloaded zip file to make sure they match. Specifically, the checksum value appears the file with the sha256 file extension. If the values do not match, the file has been corrupted somehow.

**NOTE**

Running the **Show Checksums** option may take several minutes, depending on the number and size of the patches.

6. Following these steps to confirm that the upgrade has been successfully applied:
  - a. Navigate to **Configuration, Upgrade**, and confirm that the **Upgrade History** section shows the file name that you uploaded, with the current time and date.
  - b. Navigate to **Sessions, Logs** and confirm that you can see entries for the successful upgrade and reboot of the appliance.
7. Log in to the appliance and confirm that all data is restored.

## Third-Party License Acknowledgments

---

This product includes the following third-party components. To review a complete list of these third-party components, their subcomponents, and associated license agreements, select [this link](#).



- Activation 1.1.1
- adal4j 1.1.2
- Adoptium (Temurin) Java JDK 1.8.0\_402-b06
- Adoptium (Temurin) Java JDK 11.0.22+7
- Adoptium (Temurin) Java JDK 17.0.10\_7
- Aespipe 2.4e aespipe
- Amazon AWS SDK for PHP 3.263.2
- animal-sniffer-annotations 1.1.4
- animal-sniffer-annotations 1.17
- Antlr 2.7.6
- aopalliance-repackaged 2.5.0-b42
- Apache ActiveMQ 5.16.7
- Apache ActiveMQ 5.18.3
- Apache Commons Text 1.9
- Apache Directory LDAP API 1.0.0-M20
- Apache HTTP Web Server 2.2.9
- ASM 3.1
- AutoIT 3.3.10
- AWS SDK for Java 1.12.440
- backo-java 1.0.0
- Bcpkix-jdk15on-151.jar 1.5.1
- Beanshell 2.0b6
- Boost 1.68.0
- Boost 1.73.0
- Bouncy Castle 1.56
- Bouncy Castle Java FIPS 1.0.0
- Bouncy Castle Java FIPS 1.0.1
- Bouncy Castle Java bc-fips-1.0.2
- Bouncy Castle Java bc-fips-1.0.2.4
- Bouncy Castle PKIX/CMS/EAC/PKCS/OCSP/TSP/OPENSSL 1.55
- Byte-buddy 1.6.14
- C3p0 0.9.5
- checkerframework 2.5.2
- Cliche 110413
- com.google.guava 27.0.1-jre
- com.segment.analytics.java:analytics 2.1.1
- Commons beanutils 1.9.2
- Commons Cli 1.3.1
- Commons Codec 1.7, 1.9, 1.10
- Commons Collections 4.1, 3.2.2
- Commons configuration 1.10
- Commons Digester 1.6
- Commons Discovery 0.5
- Commons FileUpload 1.3.2
- Commons Lang 2.6, 3.3.2
- Commons Logging 1.2
- Commons net 3.3
- Commons Pool 2.4.2, 1.6
- Commons-dbcp 2.2.1.1, 2.2.1, 2.5.0
- Commons-el.jar 1
- Commons-exec 1.3
- Commons-io 2.4
- Commons-lang3 3.11, 3.2.1
- Commons-net 3.6

- Apache Software License, Version 1.1
- Apache License, Version 2.0, January 2004
- Common Development and Distribution License (CDDL -Version 1.0)
- Common Development and Distribution License (CDDL -Version 1.1)
- Common Public License Version 1.0
- Eclipse Distribution License - v 1.0
- Eclipse Public License - v 1.0
- GNU General Public License, Version 2
- GNU Lesser General Public License, Version 2.1
- GNU Lesser General Public License, Version 3
- GNU General Public License, Artistic License
- IBM Public License Version 1.0
- Mozilla Public License Version 1.1
- Mozilla Public License, Version 2.0
- OpenSSL License
- Original SSLeay License
- PHP License, version 3.01
- SUN License

## Product Accessibility Features

---

Broadcom is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks.

You can use the following accessibility features with Privileged Access Manager:

### **Product Enhancements**

Privileged Access Manager offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse
- Custom Controls (if any)

#### ***Display***

To increase visibility on your computer display, you can adjust the following options:

- **Font style, color, and size of items** Defines font color, size, and other visual combinations.
- **Screen resolution** Defines the pixel count to enlarge objects on the screen.
- **Cursor width and blink rate** Defines the cursor width or blink rate, which makes the cursor easier to find or minimize its blinking.
- **Icon size** Defines the size of icons. You can make icons larger for visibility or smaller for increased screen space.
- **High contrast schemes** Defines color combinations. You can select colors that are easier to see.

#### ***Sound***

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

- **Volume** Sets the computer sound up or down.
- **Text-to-Speech** Sets the computer's hear command options and text read aloud.
- **Warnings** Defines visual warnings.
- **Notices** Defines the aural or visual cues when accessibility features are turned on or off.
- **Schemes** Associates computer sounds with specific system events.
- **Captions** Displays captions for speech and sounds.

#### ***Keyboard***

You can make the following keyboard adjustments:

- **Repeat Rate** Defines how quickly a character repeats when a key is struck.
- **Tones** Defines tones when pressing certain keys.
- **Sticky Keys** Defines the modifier key, such as Shift, Ctrl, Alt, or the Windows Logo key, for shortcut key combinations. Sticky keys remain active until another key is pressed.

#### ***Mouse***

You can use the following options to make your mouse faster and easier to use:

- **Click Speed** Defines how fast to click the mouse button to make a selection.
- **Click Lock** Sets the mouse to highlight or drag without holding down the mouse button.
- **Reverse Action** Sets the reverse function that is controlled by the left and right mouse keys.
- **Blink Rate** Defines how fast the cursor blinks or if it blinks at all.
- **Pointer Options** Lets you complete the following actions:
  - Hide the pointer while typing
  - Show the location of the pointer
  - Set the speed that the pointer moves on the screen
  - Select the size and color of the pointer for increased visibility
  - Move the pointer to a default location in a dialog

### **Keyboard Shortcuts**

The PAM Client login dialog supports the following keyboard shortcuts:

Keyboard	Description
Tab or Ctrl+Tab	Move forward through options
Shift+Tab or Ctrl+Shift+Tab	Move backward through options
Arrow keys	Move focus or selection in a group of controls, items, or tabs
Space	Locate new selection and anchor for the item.
Enter	Carry out the default command of the dialog or command of the selected control

The Privileged Access Manager UI supports the following keyboard shortcuts:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+V	Paste
Ctrl+F	Search

## Important Links

---

This content provides links to the following important information:

- The latest documentation for all supported versions of PAM is available online at <http://techdocs.broadcom.com/pam>. The site opens at the latest product version. Use the **Version** drop-down menu in the title bar near the top of the screen to access the documentation for other supported PAM versions
- [Privileged Access Manager solutions and patches](#) web page
- Free PAM education videos are available from the [IMS Software Academy](#) site.
- The 4.1 third-party license acknowledgments are available at: <https://techdocs.broadcom.com/us/en/symantec-security-software/identity-security/privileged-access-manager/4-1-1/third-party-license-acknowledgments.html>

## Telemetry Data

Broadcom uses a unique Portfolio License Agreement (PLA) model that enables customers to derive a value from the adoption and usage of the Broadcom product portfolio. Telemetry serves as the foundational data for Broadcom to measure portfolio consumption by a customer under a PLA. Telemetry is mandatory for customers participating in the PLA subscription model to enable the telemetry service and transmit usage information to the Broadcom data warehouse. This can be accomplished by using the Broadcom standalone **Product Usage Reporter** utility that is equipped with the telemetry usage reporting capabilities. The utility is a browser-based application that can be installed as a service on a Windows or a Linux machine.

For information about the Product Usage Reporter utility and its installation procedure, see [Product Usage Reporter Overview](#) and [Installing Product Usage Reporter](#).

### What Usage Data Do We Collect?

The Product Usage Reporter utility collects the following PAM data.

Data	Description
<b>Instance ID</b>	The instance ID of the product.
<b>Product usage</b>	Reports the number of devices, by type, in use on a particular day. Device types include: Access, Password Management, and A2A. If you have a cluster, the product usage data must be only from the primary site.
<b>System configuration</b>	Specifies the product version.
<b>Date when the data is collected</b>	The date when the product usage data is captured.

#### WARNING

The utility does not collect Personally Identifiable Information (PII). For more information, see [Privacy Policy](#).

### How to Configure PAM to Collect and Submit Usage Data to Us

As an administrator, configure telemetry after installing or upgrading the product.

#### Follow these steps:

1. In the UI, select **Configuration, Licensing, Telemetry Data**.
2. Complete the following fields:
  - **Is this install or upgrade related to a new or additional planned usage related to a portfolio license agreement (PLA):** If the product is installed or upgraded as part of a portfolio license agreement (PLA), select Yes. Otherwise, select No.
  - **Company Domain:** Enter your company domain name, for example, `forwardinc.com`.
  - **Enterprise Site ID:** Enter the assigned numeric ID for your organization. You can find this number on your PLA or on the [Broadcom Support site](#). To locate the number on the Support site:
    - a. Sign in to your Support account.
    - b. Select **My Account, Profile**.

- c. Under **Support Access Information**, refer to the **Site ID**.
  - **Internal Identifier:** Enter a label that identifies which group is reporting usage. Your company might have different divisions, each with their own product installations. This field enables you to indicate which division is sending data.
  - **Manually upload telemetry data:** Leave the default setting (**Yes**), to manually collect and submit the product usage data to Broadcom. A report is *not* sent automatically from the appliance.
  - **Use a proxy to send usage data:** If your appliance sits behind a proxy server, identify the server so that data can reach the telemetry service. Specify the URI of the proxy server and its associated credentials. To review proxy errors, go to Sessions, Logs page.
3. Select **Save** to complete the configuration. If you modify the telemetry configuration, always save your changes.

### **How to View and Download Usage Data for Manual Reporting**

The product usage data is saved in a file once it is submitted to Broadcom. For information about viewing and downloading the file, see [Dashboard](#).

For additional information about using or troubleshooting the utility, see [Product Usage Reporter](#).

### **How do you know if the usage data was successfully sent to us?**

View the submitted product usage data in the **Dashboard** page of the Product Usage Reporter utility. For information about viewing the usage data, see [Dashboard](#).

---

## Documentation Legal Notice

---

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The check mark in a Circle design is the registered trademark of NortonLifeLock Inc. and is used under license therefrom.

The manufacturer of this Documentation is Broadcom Inc.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.



